Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE: IBCA/P11407

CALL-OFF TITLE: **Infected Blood Compensation Authority (IBCA) - IBSS Discovery Workpackage**

CALL-OFF CONTRACT **IBSS Discovery Workpackage**

DESCRIPTION: **Contract for the provision of IBCA IBSS Discovery Workpackage**

THE BUYER: **Infected Blood Compensation Authority**

BUYER ADDRESS **Infected Blood Compensation Authority**

Benton Park View, Newcastle upon Tyne, NE7 7EB

THE SUPPLIER: **Informed Solutions Ltd**

SUPPLIER ADDRESS: The Old Bank, Old Market Place

Altrincham, Cheshire

WA14 4PA

United Kingdom

REGISTRATION NUMBER: 02755304

DUNS NUMBER: 346179542

SID4GOV ID: [**N/A**]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated **10th July 2025** .

It's issued under the Framework Contract with the reference number RM6263 for the provision of Digital Specialists and Programmes Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first Statement of Work which shall be executed at the same time that the Call-Off Contract is executed, oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

CALL-OFF LOT(S):
LOT2

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions) RM6263
3. Framework Special Terms

4. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6263
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors) - NOT USED

- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 8 (Guarantee) - NOT USED
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)
- Joint Schedule 12 (Supply Chain Visibility) - NOT USED
- Joint Schedule 13 (Cyber Essentials)

- Call-Off Schedules for RM6263
  - Call-Off Schedule 1 (Transparency Reports)
  - Call-Off Schedule 2 (Staff Transfer) - NOT USED
  - Call-Off Schedule 3 (Continuous Improvement)
  - Call-Off Schedule 5 (Pricing Details and Expenses Policy)
  - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliveries)
  - Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - Call-Off Schedule 9 (Security)
  - Call-Off Schedule 10 (Exit Management)
  - Call-Off Schedule 12 (Clustering) - NOT IN USED
  - Call-Off Schedule 13 (Implementation Plan and Testing)
  - Call-Off Schedule 14A (Service Levels)
  - Call-Off Schedule 15 (Call-Off Contract Management)
  - Call-Off Schedule 16 (Benchmarking) -
  - Call-Off Schedule 17 (MOD Terms) - NOT USED
  - Call-Off Schedule 18 (Background Checks)
  - Call-Off Schedule 19 (Scottish Law)- NOT USED
  - Call-Off Schedule 20 (Call-Off Specification)
  - Call-Off Schedule 21 (Northern Ireland Law)- NOT USED
  - Call-Off Schedule 23 (HMRC Terms) - NOT USED
  - Call-Off Schedule 25 (Ethical Walls Agreement) - NOT USED
  - Call-Off Schedule 26 (Secondment Agreement Template) - NOT USED

5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility) RM6263
7. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract: [None]

CALL-OFF START DATE:	**10th July 2025**
CALL-OFF EXPIRY DATE:	**20th August 2025**
CALL-OFF INITIAL PERIOD:	**six (6) weeks**
CALL-OFF OPTIONAL EXTENSION PERIOD:	**up to three (3) weeks**
MINIMUM NOTICE PERIOD FOR EXTENSION(S):	**one (1) week**
CALL-OFF CONTRACT VALUE:	**£185,000 (excl. VAT)**
KEY SUB-CONTRACT PRICE:	**N/A**

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)]. The Supplier agrees that the Call-Off Deliverables and associated services are to be provided in response to the Buyers Call-Off Schedule 20, and the Buyer agrees to the approach proposed by the Supplier (in Annex 3: Supplier Approach) for providing the Call-Off Deliverables and associated services, as amended during inception to take account of a later contract award and project start date. Any changes required to the Call-Off Deliverables and associated services during the performance of the Call-Off Contract will be agreed in writing between the Buyer and Suppliers Senior Delivery Manager.

BUYER's STANDARDS

From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards set out in Framework Schedule 1 (Specification). The Buyer requires the Supplier to comply with the following additional Standards for this Call-Off Contract:

As set out in the Statement of Requirements

CYBER ESSENTIALS SCHEME

The Buyer requires the Supplier, in accordance with Joint Schedule 13 (Cyber Essentials Scheme) to provide a Cyber Essentials Plus Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms, as amended by the Framework Award Form Special Terms.

The Estimated Charges used to calculate liability in this Contract Year is **REDACTED TEXT under FOIA Section 43(2), Commercial Interests.**

CALL-OFF CHARGES

Summarise the Charging method(s) Buyer has selected below and which are incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) for further details.

Firm Price based on Milestones

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

REDACTED TEXT under FOIA Section 43(2), Commercial Interests.

BUYER'S INVOICE ADDRESS:

REDACTED TEXT under FOIA Section 40, Personal Information.

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED TEXT under FOIA Section 40, Personal Information.

BUYER'S ENVIRONMENTAL POLICY

Provided on request.

BUYER'S SECURITY POLICY

Detailed in Annex 1

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED TEXT under FOIA Section 40, Personal Information

SUPPLIER'S CONTRACT MANAGER

REDACTED TEXT under FOIA Section 40, Personal Information.

PROGRESS REPORT FREQUENCY

Weekly: Weekly reporting setting out progress against key milestones and targets, schedule to be confirmed during mobilisation based on agreed terms of reference and team availability.

PROGRESS MEETING FREQUENCY

Weekly meetings (personnel to be agreed) to review weekly reports and progress.

KEY STAFF

REDACTED TEXT under FOIA Section 40, Personal Information.

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION

As per Joint Schedule 4

BALANCED SCORECARD

N/A

MATERIAL KPIs

The following Material KPIs shall apply to this Call-Off Contract in accordance with Call-Off Schedule 14A (Service Levels):

KPI/SLA	Service Area	KPI/SLA description	Target
1	Mobilisation	The lead time to onboard resources for implementation	100% of the resources onboarded within five (5) working days from contract award
2	Quality	Deliverables completed on-time and the relevant standard issued under this contract	100% of the deliverables completed on time and meeting acceptance criteria

ADDITIONAL INSURANCES
Not Applicable

GUARANTEE
Not Applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments as set out in Call-off Schedule 20 (Specification).

STATEMENT OF WORKS
During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	**REDACTED TEXT under FOIA Section 40, Personal Information**	Signature:	**REDACTED TEXT under FOIA Section 40, Personal Information**
Name:	**REDACTED TEXT under FOIA Section 40, Personal Information**	Name:	**REDACTED TEXT under FOIA Section 40, Personal Information**
Role:	**REDACTED TEXT under FOIA Section 40, Personal Information**	Role:	**REDACTED TEXT under FOIA Section 40, Personal Information**
Date:	07/07/2025	Date:	10/07/2025

Appendix 1

[**Insert** The first Statement(s) of Works shall be inserted into this Appendix 1 as part of the executed Order Form. Thereafter, the Buyer and Supplier shall complete and execute Statement of Works (in the form of the template Statement of Work in Annex 1 to the Order Form in Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)].

[**Insert** Each executed Statement of Work shall be inserted into this Appendix 1 in chronology.]

Annex 1 (Template Statement of Work)

1. STATEMENT OF WORK ("SOW") DETAILS	
Upon execution, this SOW forms part of the Call-Off Contract (reference below). The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW. All SOWs must fall within the Specification and provisions of the Call-Off Contact. The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.	
Date of SOW:	
SOW Title:	
SOW Reference:	

Call-Off Contract Reference:	
Buyer:	
Supplier:	
SOW Start Date:	

SOW End Date:	
Duration of SOW:	
Key Personnel (Buyer)	
Key Personnel (Supplier)	
Subcontractors	

2. CALL-OFF CONTRACT SPECIFICATION - PROGRAMME CONTEXT	
SOW Deliverables Background	*[Insert details of which elements of the Deliverables this SOW will address].*
Delivery phase(s)	*[Insert item and nature of Delivery phase(s), for example, Discovery, Alpha, Beta or Live].*
Overview of Requirement	*[Insert details including Release Types(s), for example, Adhoc, Inception, Calibration or Delivery].*
Accountability Models	*Please tick the Accountability Model(s) that shall be used under this Statement of Work:* *Sole Responsibility:*☐ *Self Directed Team:*☐ *Rainbow Team:*☐

3. BUYER REQUIREMENTS – SOW DELIVERABLES	
Outcome Description	

Milestone Ref	Milestone Description	Acceptance Criteria	Due date

Key Role	Key Staff	Contract Details

MS01			
MS02			
Delivery Plan			
Dependencies			
Supplier Resource Plan			

Security Applicable to SOW:	The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security). **[**If different security requirements than those set out in Call-Off Schedule 9 (Security) apply under this SOW, these shall be detailed below and apply only to this SOW: *[insert if necessary]* **]**
Cyber Essentials Scheme	The Buyer requires the Supplier to have and maintain a Cyber Essentials Plus Certificate for the work undertaken under this SOW, in accordance with Joint Schedule 13 (Cyber Essentials Scheme).
SOW Standards	[Insert any specific Standards applicable to this SOW (check Annex 3 of Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules)]
Performance Management	[Insert details of Material KPIs that have a material impact on Contract performance] [Insert Service Levels and/or KPIs – See Call-Off Schedule 14 (Service Levels and Balanced Scorecard)]
Additional Requirements	**Annex 1 –** Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex 1 attached to this Statement of Work.
Key Supplier Staff	[Indicate: whether there is any requirement to issue a Status Determination Statement]

Worker Engagement Status	[Yes / No] [Insert details]

[SOW Reporting Requirements:]	**[**Further to the Supplier providing the management information detailed in Call-Off Schedule 15 (Call-Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only: **]**

4. CHARGES	
Call Off Contract Charges	The applicable charging method(s) for this SOW is: · [Capped Time and Materials] · [Incremental Fixed Price] · [Time and Materials] · [Fixed Price] · [2 or more of the above charging methods] ***[Buyer to select as appropriate for this SOW]*** The estimated maximum value of this SOW (irrespective of the selected charging method) is £[Insert detail]. The Charges detailed in the financial model shall be invoiced in accordance with Clause 4 of the Call-Off Contract.
Rate Cards Applicable	***[Insert** SOW applicable Supplier and Subcontractor rate cards from Call-Off Schedule 5 (Pricing Details and Expenses Policy), including details of any discounts that will be applied to the work undertaken under this SOW.]*
Financial Model	*[Supplier to insert its financial model applicable to this SOW]*
Reimbursable Expenses	[See Expenses Policy in Annex 1 to Call-Off Schedule 5 (Pricing Details and Expenses Policy)] [Reimbursable Expenses are capped at [£[Insert] [**OR** [**Insert**] percent ([X]%) of the Charges payable under this Statement of Work.] [None] *[Buyer to delete as appropriate for this SOW]*

5. SIGNATURES AND APPROVALS

Agreement of this SOW BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the

Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:	
For and on behalf of the Supplier	Nam e and title Date Signature
For and on behalf of the Buyer	Name and title Date Signature

ANNEX 2: Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority 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 Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: - Full name - Name of employer - Job title - Pay **NB**: the scope of this engagement means that the Supplier will not, under any circumstances, have a need to gather personal data that belongs to IBSS' service users. The personal data types listed above are pertinent to IBSS' staff only and will be gathered, primarily, through user research activity.
Duration of the Processing	14.07.2025 - 20.08.2025 inclusive
Nature and purposes of the Processing	Data will be collected, primarily, through user research interviews between the supplier and IBSS' staff. Interviews will, with the participant's permission, be recorded and a transcript captured. Participant consent to IBCA's processing of their personal data will be captured in the recording and recorded on a content log, which the Supplier will set up and maintain. These artefacts will be used to inform summary documents from each interview, trend analysis across all user research activity and, ultimately, inform the Discovery report that the Supplier will provide to IBCA at the end of the engagement. All user research artefacts will be stored on IBCA's instance of AO Docs.
Type of Personal Data	- Full name - Employer - Job title - Pay

Categories of Data Subject	Staff employed by the following organisations: **REDACTED TEXT under FOIA Section 40, Personal Information**
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 dataunder Union or Member State law to preserve that type of data**	In-keeping with IBCA's policy for the destruction of data gathered through user research for the core service, data will be destroyed a maximum of 18 months after processing is complete (unless the data subject requests this to be done sooner).

ANNEX 3: Supplier Approach

REDACTED TEXT under FOIA Section 43(2), Commercial Interests.

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the contract):

Contract Details

This variation is between: [delete as applicable: CCS / Buyer] ("CCS" / "the Buyer") And
[insert name of Supplier] ("the Supplier")

Contract name: [insert name of contract to be changed] ("the Contract")

Contract reference number: [insert contract reference number]

[Statement of Work (SOW) reference:]

[insert SOW reference number and title (if applicable) or delete row]

[Buyer reference:] [insert cost centre/portfolio codes as appropriate]
Details of Proposed Variation
Variation initiated by: [delete as applicable: CCS/Buyer/Supplier]
Variation number: [insert variation number]
Date variation is raised: [insert date]
Proposed variation [insert detail here or use Annex 1 below] Reason for the variation: [insert reason]

An Impact Assessment shall be provided within:

[insert number] days

Likely impact of the proposed variation:

Impact of Variation

[Supplier to insert assessment of impact]

Outcome of Variation

Contract variation: This Contract detailed above is varied as follows:

- [CCS/Buyer to insert original Clauses or Paragraphs to be varied and the changed clause]

- [reference Annex 1 as appropriate]

Financial variation: Original Contract Value: £ [insert amount]
Additional cost due to variation: £ [insert amount] New Contract value:
£ [insert amount]
[Timescale variation/s:] [insert changes to dates/milestones or delete row]

Model Version:

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by [delete as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract. The 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 [delete as applicable: CCS / Buyer]

Signature

Date

Name (in capitals)

Job Title

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in capitals)

Job Title

Address

ANNEX 1

[insert details as required]

Joint Schedule 3 (Insurance Requirements)

1. The insurance the Supplier needs 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, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("Additional Insurances") 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:

1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

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 the Contract Period and 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 Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority 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. What Certification do you need

2.1 Without limiting the other provisions of this 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.

evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if the Supplier is not 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 Relevant Authority 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 to be provided

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 Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Required amount of insurance

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 Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or nonrenewal 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 Relevant Authority (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 each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority 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 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 Relevant Authority) 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 Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following insurance cover from the Framework 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 and products 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).

Joint Schedule 4 (Commercially Sensitive Information)

1. **What is the Commercially Sensitive Information?**

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

Date	Items	Duration of Confidentiality
10.07.2025	Pricing	Contract Term

Joint Schedule 7 (Financial Difficulties)

1. Definitions

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

"Credit Rating Threshold" the minimum credit rating level for the Monitored Company as set out in Annex 2 and

"Financial Distress Event" the occurrence or one or more of the following events:

a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold;

b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;

c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Company;

d) Monitored Company committing a material breach of covenant to its lenders;

e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or

f) any of the following:

i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;

ii) non-payment by the Monitored Company of any financial indebtedness;

iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or

iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company

in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;

"Financial Distress Service Continuity Plan" a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;

"Monitored Company" Supplier [Guarantor] or any Key Subcontractor]

"Rating Agencies" the rating agencies listed in Annex 1.

2. **When this Schedule applies**

2.1The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Schedule shall survive:

2.2.1 under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

2.2.2 under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

3. **What happens when your credit rating changes**

3.1The Supplier warrants and represents to CCS that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within five (5) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.

3.3 If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with sufficient working accounts to allow further validation of financial status to be undertaken.

[Guidance: check with Commercial Finance what provisions to make here]

3.4 **The Supplier shall:**

3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and

3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS and Buyers in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or

matter which could cause a Financial Distress Event.

3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. **What happens if there is a financial distress event**

4.1In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

[Guidance: delete this clause if there are no Key Subcontractors or the Key Subcontractors are not Monitored Company]

4.2[In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.]

4.3The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1 at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the

continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2 where CCS or Buyers reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1 which CCS may share with Buyers) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

(a) submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and

(b) provide such financial information relating to the Monitored Company as CCS may reasonably require.

4.4If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

4.5If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

4.6Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;

4.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

4.6.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

4.7Where the Supplier reasonably believes that the relevant Financial Distress

Event (or the circumstance or matter which has caused or otherwise led to it)

no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.

4.8CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

5. When CCS or the Buyer can terminate for financial distress

5.1CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5;

5.1.3 in the case of the Buyer, the Supplier fails to agree a Financial Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) that ensures the continued performance of the Contract and delivery of the Deliverables under its Contract; and/or

5.1.4 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

6. What happens If your credit rating is still good

6.1Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

ANNEX 1: RATING AGENCIES

Dun and Bradstreet (“D&B”)

[Rating Agency 2]

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (long term)
Supplier	[D&B Threshold]
[Guarantor]	
[Key Subcontractor]	

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan

Details of the Default: [Guidance: Explain the Default, with clear Schedule, Clause and Paragraph references as appropriate]

Deadline for receiving the [Revised] Rectification Plan:

[add date (minimum 10 days from request)]

Signed by [CCS/Buyer] : Date:

Supplier [Revised] Rectification Plan

Cause of the Default [add cause]

Anticipated impact assessment:

[add impact]

Actual effect of Default: [add effect]

Steps to be taken to rectification:

Timescale for complete rectification of Default

Steps	Timescale
1.	[date]
2.	[date]
3.	[date]
4.	[date] […] [date] [X] Working Days

Steps taken to prevent recurrence of Default

Steps	Timescale
1.	[date]

2. [date]

3. [date]

4. [date]

[…] [date]

Signed by the Supplier: Date:

Review of Rectification Plan [CCS/Buyer]

Outcome of review [Plan Accepted] [Plan Rejected] [Revised Plan Requested]

Reasons for rejection (if applicable)

[add reasons]

Signed by [CCS/Buyer] Date:

Joint Schedule 11 (Processing Data)

Definitions

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

"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. 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 2018. 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

3. 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.

4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5. 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 Deliverables;

(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.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the 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 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 Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

(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 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 UK or 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 UK 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 Contract unless the Processor is required by Law to retain the Personal Data.

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the 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 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.

8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

9. 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 7 of this Joint Schedule 11 (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.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. 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 UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Subprocessor to Process any Personal Data related to the 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 Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 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 Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the 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

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. 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.

19. 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.

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 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.

21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

22. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the 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 UK GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

23. 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 UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with

Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25. 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 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.

26. 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 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.

27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 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 paragraphs 18 to 28 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

[Please refer to Annex 2 Data Processing of the Order Form for the table]

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 Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**

1.2 The contact details of the Supplier's Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**

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.

Annex 2 - Joint Controller Agreement

N/A

Joint Schedule 13 (Cyber Essentials Scheme)

1. Definitions

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

- "Cyber Essentials Scheme" the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found at: https://www.cyberessentials.ncsc.gov.uk/
- "Cyber Essentials Basic Certificate" the certificate awarded on the basis of selfassessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;
- "Cyber Essentials Certificate" Cyber Essentials Basic Certificate or the Cyber Essentials Plus Certificate to be provided by the Supplier as set out in the Order Form
- "Cyber Essential Scheme Data" sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
- "Cyber Essentials Plus Certificate" the certification awarded on the basis of external testing by an independent certification body of the Supplier's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

2. What Certification do you need

2.1 Where the Framework Award Form and/or Order Form requires that the Supplier provide a Cyber Essentials Plus Certificate prior to Framework Start Date and/or commencing the provision of Deliverables under the Call-Off Contract including, if applicable, any Statement of Work, the Supplier shall provide a valid Cyber Essentials Plus Certificate to CCS and/or the Buyer. Where the Supplier fails to comply with this Paragraph it shall be prohibited from commencing the provision of Deliverables under the Call-Off Contract until such time as the Supplier has evidenced to CCS and/or the Buyer its compliance with this Paragraph 2.1.

2.2 Where the Supplier continues to process data during the Call-Off Contract Period the Supplier shall deliver to CCS and/or the Buyer evidence of renewal of the Cyber Essentials Plus Certificate on each anniversary of the first applicable certificate obtained by the Supplier under Paragraph 2.1.

2.3 In the event that the Supplier fails to comply with Paragraph 2.1 or 2.2, CCS and/or the Buyer reserves the right to terminate the Call-Off Contract for material Default.

2.4 The Supplier shall ensure that all Sub-Contracts with Subcontractors who Process Cyber Essentials Data contain provisions no less onerous on the Subcontractors than those imposed on the Supplier under the Call-Off Contract in

respect of the Cyber Essentials Plus Scheme under Paragraph 2.1 of this Schedule.

2.5 This Schedule shall survive termination or expiry of this Contract and each and any Call-Off Contract.

Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Order Form lists the key roles ("Key Roles") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date and, if applicable, the Statement of Work will list the Key Roles and names of persons who the Supplier shall appoint to fill those Key Roles as of the SOW Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;
1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables;
1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced;

1.5.6 on written request from the Buyer, provide a copy of the contract of employment or engagement (between the Supplier and Supplier Staff) for every member of the Supplier Staff made available to the Buyer under the Call-Off Contract when providing Deliverables, and under each Statement of Work;
1.5.7 on written request from the Buyer, provide details of start and end dates of engagement of all Key Staff filling Key Roles under the Call-Off Contract and, if applicable, under each Statement of Work[.[; and]
1.5.8 [Insert any additional requirements].]

1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Call-Off Schedule 9 (Security)

Part A : Short-form Security Requirements

[Please note that Part A has been replaced by Cabinet Office Security Requirements as per Annex 1]

Annex 1 Security Management

1 SUPPLIER OBLIGATION

1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 8.

1.2 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Certifications (see Paragraph 4)		
The Supplier must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS- recognised Certification Body	☒
	Cyber Essentials Plus	☒
	Cyber Essentials	☐
	No certification required	☐
Subcontractors that Handle Government Data must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☐
	Cyber Essentials Plus	☒
	Cyber Essentials	☐
	No certification required	☐
Locations (see Paragraph 5)		

The Supplier and Subcontractors may store, access or Handle Government Data in:	the United Kingdom only	☒
	a location permitted by and in accordance with any regulations for the time being in force made under 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	☐
	anywhere in the world not prohibited by the Buyer	☐
Staff Vetting Procedure (see Paragraph 6)		
The Buyer requires a Staff Vetting Procedure other than BPSS		☒

Optional requirements

1.3 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding Paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

Cloud Security Principles (see Paragraph 10)	
The Supplier must assess the Supplier System against the Cloud Security Principles	☐

Record keeping (see Paragraph 11)	
The Supplier must keep records relating to Subcontractors, Sites, Third-Party Tools and third parties	☒
Encryption (see Paragraph 12)	

The Supplier must encrypt Government Data while at rest or in transit	☒
Protective Monitoring System (see Paragraph 13)	
The Supplier must implement an effective Protective Monitoring System	☒
Patching (see Paragraph 14)	
The Supplier must patch vulnerabilities in the Supplier System promptly	☒
Malware protection (see Paragraph 15)	
The Supplier must use appropriate Anti-virus Software	☒
End-User Devices (see Paragraph 16)	
The Supplier must manage End-User Devices appropriately	☒
Vulnerability scanning (see Paragraph 17)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	☒
Access control (see Paragraph 18)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	☒
Remote Working (see Paragraph 19)	
The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place	☐
Backup and recovery of Government Data (see Paragraph 20)	
The Supplier must have in place systems for the backup and recovery of Government Data	☐
Return and deletion of Government Data (see Paragraph 21)	

The Supplier must return or delete Government Data when requested by the Buyer	☒
Physical security (see Paragraph 22)	
The Supplier must store Government Data in physically secure locations	☒
Security breaches (see Paragraph 23)	
The Supplier must report any Breach of Security to the Buyer promptly	☒

2 DEFINITIONS

"Anti-virus Software"	means software that:	
	(a)	protects the Supplier System from the possible introduction of Malicious Software;

(b) scans for and identifies possible Malicious Software in the Supplier System;

(c) if Malicious Software is detected in the Supplier System, so far as possible:

(i) prevents the harmful effects of the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System;

"BPSS" means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as that document is updated from time to time;

"Breach of Security" means the occurrence of:

(a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;

(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or

(c) any part of the Supplier System ceasing to be compliant with the required Certifications;

(d) the installation of Malicious Software in the Supplier System:

(e) any loss of operational efficiency or failure to operate to specification as the result of the

installation or operation of Malicious Software in the Supplier System; and

(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:

(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or

(ii) was undertaken, or directed by, a state other than the United Kingdom;

"Buyer Equipment"	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
"Buyer Security Policies"	means those securities specified by the Buyer in Paragraph 1.3;
“Buyer System”	means the Buyer's information and communications technology system, including any software or Buyer Equipment, owned by the Buyer or leased or licenced to it by a third-party, that: (a) is used by the Buyer or Supplier in connection with this Contract; (b) interfaces with the Supplier System; and/or (c) is necessary for the Buyer to receive the Services.
“Certifications”	means one or more of the following certifications (or equivalent): (a) ISO/IEC 27001:2022 by a UKAS- recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and

(b) Cyber Essentials Plus; and/or

(c) Cyber Essentials;

"CHECK Scheme" means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;

"CHECK Service Provider" means a company which, under the CHECK Scheme:

(a) has been certified by the NCSC;

(b) holds "Green Light" status; and

(c) is authorised to provide the IT Health Check services required by Paragraph 9.2 (*Security Testing*);

"Cloud Security Principles" means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles;

"Contract Year" means:

14.9.1 a period of 12 months commencing on the Start Date;

14.9.2 thereafter a period of 12 months commencing on each anniversary of the Start Date;

(a) with the final Contract Year ending on the expiry or termination of the Term;

"CREST Service Provider" means a company with an information security accreditation of a security operations centre qualification from CREST International;

"Cyber Essentials" means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;

“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the NCSC;
“Developed System”	means the software or system that the Supplier is required to develop under this Contract;
“End-User Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
"Expected Behaviours"	means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html;
“Government Data”	Means any: . (a) data, texts, 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; (b) Personal Data for which the Buyer is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in Paragraphs (a) or (b); that is: (d) supplied to the Supplier by or on behalf of the Buyer; or (e) that the Supplier is required to generate, Process, Handle, store or transmit under this Contract;

"Government Security Classification Policy"	means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications;
"Handle"	means any operation performed on data, whether or not by automated means, including 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 that data;
"IT Health Check"	means the security testing of the Supplier System;
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC"	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"Privileged User"	means a user with system administration access to the Supplier System, or substantially similar access privileges;
"Prohibition Notice"	means the meaning given to that term by Paragraph 4.4.
"Protective Monitoring System"	has the meaning given to that term by Paragraph 13.1;

“Relevant Conviction”	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
"Remote Location"	means [the relevant Supplier Staff's permanent home address authorised by the Supplier or Sub-contractor (as applicable) for Remote Working OR a location other than a Supplier's or a Sub-contractor's Site];
"Remote Working"	means the provision or management of the Services by Supplier Staff from a location other than a Supplier’s or a Sub-contractor’s Site;
"Remote Working Policy"	the policy prepared and approved under Paragraph 22 under which Supplier Staff are permitted to undertake Remote Working;
"Security Controls"	means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html;
“Sites”	means any premises (including the Buyer’s Premises, the Supplier’s premises or third party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where:

(i) any part of the Supplier System is situated; or

(ii) any physical interface with the Buyer System takes place;

"Staff Vetting Procedure" means the procedure for vetting Supplier Staff set out in Paragraph 6;

“Subcontractor Staff” means:

(a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and

(b) engaged in or likely to be engaged in:

(i) the performance or management of the Services; or

(ii) the provision of facilities or services that are necessary for the provision of the Services;

Supplier System” means

(a) any:

(i) information assets,

(ii) IT systems,

(iii) IT services; or

(iv) Sites,

that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, or support the provision of, the Services; and

(b) the associated information management system, including all relevant:

(i) organisational structure diagrams;

(ii) controls;

(iii) policies;

(iv) practices;

(v) procedures;

(vi) processes; and

(vii) resources;

“Third-party Tool” means any software used by the Supplier by which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;

"UKAS-recognised Certification Body" means:

(a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or

(b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment.

PART ONE: CORE REQUIREMENTS

3 HANDLING GOVERNMENT DATA

3.1 The Supplier acknowledges that it:

(a) must only Handle Government Data that is classified as OFFICIAL; and

(b) must not Handle Government Data that is classified as SECRET or TOP SECRET.

3.2 The Supplier must:

(a) not alter the classification of any Government Data.

(b) if it becomes aware that it has Handled any Government Data classified as SECRET or TOP SECRET the Supplier must:

i. immediately inform the Buyer; and

ii. follow any instructions from the Buyer concerning the Government Data.

3.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:

(a) the Expected Behaviours; and

(b) the Security Controls.

4 CERTIFICATION REQUIREMENTS

4.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Handle Government Data are certified as compliant with Cyber Essentials (or equivalent).

4.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

(a) it; and

(b) any Subcontractor that Processes Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1 (or equivalent certifications):

4.3 The Supplier must ensure that the specified Certifications (or their equivalent) are in place for it and any relevant Subcontractor:

(a) before the Supplier or any Subcontractor Handles Government Data; and

(b) throughout the Term.

5 LOCATION

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Government Data outside:

(a) the United Kingdom; or

(b) a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

5.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that all Subcontractors, at all times store, access or Handle Government Data only in or from the geographic areas specified by the Buyer.

5.3 The Supplier must, and must ensure that its Subcontractors store, access or Handle Government Data in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Subcontractors in this Annex;

(c) the Supplier or Subcontractor has taken reasonable steps to assure itself that:

(i) the entity complies with the binding agreement; and

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Subcontractor will store, access, manage and/or Process the Government Data as required by this Annex;

5.3.1 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 4.4.

5.4 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken the storage, accessing or Processing of Government Data in one or more countries or territories (a "**Prohibition Notice**").

5.5 Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

6 STAFF VETTING

6.1 The Supplier must not allow Supplier Staff, and must ensure that Subcontractors do not allow Subcontractor Staff, to access or Handle Government Data, if that person:

(a) has not completed the Staff Vetting Procedure; or

(b) where no Staff Vetting Procedure is specified in the Order Form:

i. has not undergone the checks required for the BPSS to verify:

A. the individual's identity;

B. where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom; and

C. the individual's previous employment history; and

D. that the individual has no Relevant Convictions; and

ii. national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify.

6.2 Where the Supplier considers it cannot ensure that a Sub-contractor will undertake the relevant security checks on any Sub-contractor Staff, it must:

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor staff will perform as the Buyer reasonably requires; and

(c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contract.

7 Supplier assurance letter

7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its [chief technology officer] (or equivalent officer) confirming that, having made due and careful enquiry:

(a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;

(b) it has fully complied with all requirements of this Annex; and

(c) all Subcontractors have complied with the requirements of this Annex with which the Supplier is required to ensure they comply;

(d) the Supplier considers that its security and risk mitigation procedures remain effective.

8 Assurance

8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Annex.

8.2 The Supplier must provide that information and those documents:

(a) at no cost to the Buyer;

(b) within 10 Working Days of a request by the Buyer;

(a) except in the case of original document, in the format and with the content and information required by the Buyer; and

(b) in the case of original document, as a full, unedited and unredacted copy.

9 Use of Subcontractors and third parties

9.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Handle Government Data comply with the requirements of this Annex.

PART TWO : ADDITIONAL REQUIREMENTS

10 CLOUD SECURITY PRINCIPLES

10.1 The Supplier must ensure that the Supplier System complies with the Cloud Security Principles.

10.2 The Supplier must assess the Supplier System against the Cloud Security Principles to assure itself that it complies with Paragraph 10.1:

- before Handling Government Data;
- at least once each Contract Year; and
- when required by the Buyer.

10.3 Where the Cloud Security Principles provide for various options, the Supplier must document the option it has chosen to implement and its reasons for doing do.

10.4 The Supplier must:

(a) keep records of any assessment that it makes under Paragraph 11.2; and

(b) provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

11 INFORMATION ABOUT SUBCONTRACTORS, SITES AND THIRD-PARTY TOOLS

11.1 The Supplier must keep the following records:

(a) for Subcontractors or third parties that store, have access to or Handle Government Data:

i. the Subcontractor or third party's name:

A. legal name;

B. trading name (if any); and

C. registration details (where the Subcontractor is not an individual), including:

(A) country of registration;

(B) registration number (if applicable); and

(C) registered address;

D. the Certifications held by the Subcontractor or third party;

E. the Sites used by the Subcontractor or third party;

F. the Services provided or activities undertaken by the Subcontractor or third party;

G. the access the Subcontractor or third party has to the Supplier System;

H. the Government Data Handled by the Subcontractor or third party; and

I. the measures the Subcontractor or third party has in place to comply with the requirements of this Annex;

ii. for Sites from or at which Government Data is accessed or Handled:

A. the location of the Site;

B. the operator of the Site, including the operator's:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual);

C. the Certifications that apply to the Site;

D. the Government Data stored at, or Handled from, the site; and

iii. for Third-party Tools:

A. the name of the Third-Party Tool;

iv. the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and

A. in respect of the entity providing the Third-Party Tool, its:

(A) full legal name;

(B) trading name (if any)

(C) country of registration;

(D) registration number (if applicable); and

(E) registered address.

11.2 The Supplier must update the records it keeps in accordance with Paragraph 11.1:

(a) at least four times each Contract Year;

(b) whenever a Subcontractor, third party that accesses or Handles Government Data, Third-party Tool or Site changes; or

(c) whenever required to go so by the Buyer.

11.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 11.1 to the Buyer within 10 Working Days of any request by the Buyer.

12 **Encryption**

12.1 The Supplier must, and must ensure that all Subcontractors, encrypt Government Data:

- when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
- when transmitted.

13 Protective monitoring system

13.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

(a) identify and prevent any potential Breach of Security;

(b) respond effectively and in a timely manner to any Breach of Security that does;

(c) identify and implement changes to the Supplier System to prevent future any Breach of Security; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

(the "**Protective Monitoring System**").

The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier System; and

(b) regular reports and alerts to identify:

i. changing access trends;

ii. unusual usage patterns; or

iii. the access of greater than usual volumes of Government Data; and

iv. the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

14 PATCHING

14.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

(a) the Supplier must patch any vulnerabilities classified as "**critical**":

v. if it is technically feasible to do so, within 5 Working Days of the public release; or

vi. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(a)(i), then as soon as reasonably practicable after the public release;

(b) the Supplier must patch any vulnerabilities classified as "**important**":

i. if it is technically feasible to do so, within 1 month of the public release; or

ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(b)(i), then as soon as reasonably practicable after the public release;

(c) the Supplier must remedy any vulnerabilities classified as "**other**" in the public release:

i. if it is technically feasible to do so, within 2 months of the public release; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 17.1(c)(i), then as soon as reasonably practicable after the public release;

(d) where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

15 MALWARE PROTECTION

15.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

15.2 The Supplier must ensure that such Anti-virus Software:

(a) prevents the installation of the most common forms of Malicious Software in the Supplier System;

(b) performs regular scans of the Supplier System to check for Malicious Software; and

(c) where Malicious Software has been introduced into the Supplier System, so far as practicable

iii. prevents the harmful effects from the Malicious Software; and

iv. removes the Malicious Software from the Supplier System.

16 END-USER DEVICES

16.1 The Supplier must, and must ensure that all Subcontractors, manage all End-User Devices on which Government Data is stored or Handled in accordance with the following requirements:

(a) the operating system and any applications that store, Handle or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Government Data must be encrypted using a suitable encryption tool;

(d) the End-User Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-User Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;

(f) the Supplier or Subcontractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Government Data stored on the device and prevent any user or group of users from accessing the device;

(g) all End-User Devices are within the scope of any required Certification.

16.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.

17 VULNERABILITY SCANNING

17.1 The Supplier must:

(a) scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

(b) if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 14.

18 ACCESS CONTROL

18.1 The Supplier must, and must ensure that all Subcontractors:

(a) identify and authenticate all persons who access the Supplier System before they do so;

(b) require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

(c) allow access only to those parts of the Supplier System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier System.

18.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier System:

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End-User Devices;

(c) are configured so that those accounts can only be used for system administration tasks;

(d) require passwords with high complexity that are changed regularly;

(e) automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and

(f) are:

v. restricted to a single role or small number of roles;

vi. time limited; and

vii. restrict the Privileged User's access to the internet.

19 REMOTE WORKING

19.1 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

(a) unless in writing by the Authority, Privileged Users do not undertake Remote Working;

(b) where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

19.2 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

(a) prepare and have approved by the Buyer in the Remote Working Policy in accordance with this Paragraph;

(b) undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

(c) ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;

(d) may not permit any Supplier Staff or the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

19.3 The Remote Working Policy must include or make provision for the following matters:

(a) restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

(b) restricting or prohibiting Supplier Staff from downloading any Government Data to any End-User Device other than an End User Device that:

i. is provided by the Supplier or Sub-contractor (as appropriate); and

ii. complies with the requirements set out in Paragraph 3 (*End-User Devices*);

(c) ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

(d) giving effect to the Security Controls (so far as they are applicable); and

(e) for each different category of Supplier Staff subject to the proposed Remote Working Policy:

i. the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;

ii. any identified security risks arising from the proposed Handling in a Remote Location;

iii. the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and

iv. the business rules with which the Supplier Staff must comply.

19.4 The Supplier may submit a proposed Remote Working Policy for consideration at any time.

20 BACKUP AND RECOVERY OF GOVERNMENT DATA

20.1 The Supplier must ensure that the Supplier System:

(a) backs up and allows for the recovery of Government Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and

(b) retains backups of the Government Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

20.2 The Supplier must ensure the Supplier System:

(a) uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;

(b) the backup system monitors backups of Government Data to:

i. identify any backup failure; and

ii. confirm the integrity of the Government Data backed up;

(c) any backup failure is remedied properly;

(d) the backup system monitors backups of Government Data to:

i. identify any recovery failure; and

ii. confirm the integrity of Government Data recovered; and

(e) any recovery failure is promptly remedied.

21 RETURN AND DELETION OF GOVERNMENT DATA

21.1 Subject to Paragraph 21.2, when requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

(a) securely erase any or all Government Data held by the Supplier or Subcontractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

(b) provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor using the method specified by the Buyer.

21.2 Paragraph 21.1 does not apply to Government Data:

(a) that is Personal Data in respect of which the Supplier is a Controller;

(b) to which the Supplier has rights to Handle independently from this Contract; or

(c) in respect of which, the Supplier is under an obligation imposed by Law to retain.

21.3 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor:

(a) when requested to do so by the Buyer; and

(b) using the method specified by the Buyer.

22 PHYSICAL SECURITY

22.1 The Supplier must, and must ensure that Subcontractors, store the Government Data on servers housed in physically secure locations.

23 BREACH OF SECURITY

23.1 If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

(a) notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;

(b) provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction;

(c) where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer.

Call-Off Schedule 10 (Exit Management)

1. Definitions

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

"Exclusive Assets"	Supplier Assets used exclusively by the Supplier in the provision of the Deliverables;
"Exit Information"	has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under this Schedule;
"Exit Plan"	the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule;
"Net Book Value"	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier in connection with the Deliverables but which are also used by the Supplier for other purposes;
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier in connection with the Deliverables but which are also used by the Supplier for other purposes;

"Registers"	the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
"Transferable Assets"	Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which

	are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts	has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2. Supplier must always be prepared for Contract exit and SOW exit

2.1 The Supplier shall within 30 days from the Call-Off Contract Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables' IPR asset management system which includes all Document and Source Code repositories.

("**Registers**").

2.3 The Supplier shall

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Call-Off Contract Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of each SOW and this Contract.

3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence whether this is in relation to one or more SOWs or the Call-Off Contract (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan - NOT USED

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer a Call-Off Contract and SOW Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable (this may require

modification to SOW Exit Plan provisions to be updated and incorporated as part of the SOW;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) prior to each SOW and no less than every [six (6) months] throughout the Contract Period; and

(b) no later than [twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than [ten (10) Working Days] after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than [twenty (20) Working Days] following,

any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable, in the case of the Call-Off Contract and each SOW (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels or KPI, the Parties shall vary the relevant KPIs, Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-Contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**), in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under

that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A - Implementation

1. Definitions

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

"Delay"	a) a delay in the Achievement of a Milestone by its Milestone Date; or b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
"Milestone Payment"	a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
Implementation Period"	has the meaning given to it in Paragraph 7.1;

2. Agreeing and following the Implementation Plan

2.1 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan 5 Working days after the Call-Off Contract Start Date.

2.2 The draft Implementation Plan:

2.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively for the whole Call-Off Contract and each Statement of Work issued under it for the supply of Deliverables and as the Buyer may otherwise require

2.2.2 shall provide details on how the required Social Value commitments will be delivered through the Call-Off Contract; and

2.2.3 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

2.3 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2.4 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

2.5 The Supplier shall also provide as required or requested reports to the Buyer concerning activities and impacts arising from Social Value including in the Implementation Plan.

2.6 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

2.7 The Supplier shall, in relation to each SOW, incorporate within it all Implementation Plan and Testing requirements for the satisfactory completion of each Deliverable Item to be provided under that SOW.

3. Reviewing and changing the Implementation Plan

3.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.

3.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

3.3 Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

3.4 Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

4. Security requirements before the Start Date

4.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.

4.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

4.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

4.4 The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

5. What to do if there is a Delay

5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

5.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and

5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

6. Compensation for a Delay

6.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

6.1.1 the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;

6.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:

(a) the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

(b) the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

6.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

6.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

6.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

7. Implementation Plan

7.1 The Implementation Period will be a [six (6)] Month period for the Call-Off Contract and for the duration of each SOW.

7.2 During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer in each SOW. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.

7.3 In accordance with the Implementation Plan, the Supplier shall:

7.3.1 work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where

applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;

7.3.2 work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;

7.3.3 liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and

7.3.4 produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

7.4 The Implementation Plan will include detail stating:

7.4.1 how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and

7.4.2 a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.

7.5 In addition, the Supplier shall:

7.5.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;

7.5.2 mobilise all the Services specified in the Specification within the Call-Off Contract and each SOW;

7.5.3 produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

(a) the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and

(b) the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

7.5.4 manage and report progress against the Implementation Plan both at a Call-Off Contract level (which shall include an update on costings) and SOW level;

7.5.5 construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;

7.5.6 attend progress meetings (frequency of such meetings shall be as set out in the Order Form and each SOW) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and

7.5.7 ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.

Annex 1: Implementation Plan

A.1 The Supplier shall provide a:

(a) high level Implementation Plan for the Call-Off Contract as part of the Further Competition Procedure; and

(b) a detailed Implementation Plan for each SOW.

A.2 The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

Milestone	Deliverable Items	Duration	Buyer Responsibilities	Milestone Payments	Delay Payments
Milestone 1	[]	[]			

Milestones will be Achieved in accordance with this Call-Off Schedule13: (Implementation Plan and Testing).

The purposes of Paragraph 9.1.2 the Delay Period Limit shall be **[insert number of days]** .

Part B - Testing

1. Definitions

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

"Component"	any constituent parts of the Deliverables;
"Material Test Issue"	a Test Issue of Severity Level 1 or Severity Level 2;
"Satisfaction Certificate"	a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;
"Severity Level"	the level of severity of a Test Issue, the criteria for which are described in Annex 1;
"Test Issue Management Log"	a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule;
"Test Issue Threshold"	in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Reports"	the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of this Schedule;
"Test Strategy"	a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule;
"Test Success Criteria"	in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule

"Test Witness"	any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and
"Testing Procedures"	the applicable testing procedures and Test Success Criteria set out in this Schedule.

2. How testing should work

2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.

2.2 The Supplier shall not submit any Deliverable for Testing:

2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

2.2.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and

2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

2.4 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

3. Planning for testing

3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.

3.2 The final Test Strategy shall include:

3.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;

3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

3.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;

3.2.4 the procedure to be followed to sign off each Test;

3.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;

3.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;

3.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;

3.2.8 the technical environments required to support the Tests; and

3.2.9 the procedure for managing the configuration of the Test environments.

4. Preparing for Testing

4.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.

4.2 Each Test Plan shall include as a minimum:

4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and

4.2.2 a detailed procedure for the Tests to be carried out.

4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

5. Passing Testing

5.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

6. How Deliverables will be tested

6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).

6.2 Each Test Specification shall include as a minimum:

6.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

6.2.4 Test pre-requisites and the mechanism for measuring them; and

6.2.5 expected Test results, including:

(a) a mechanism to be used to capture and record Test results; and

(b) a method to process the Test results to establish their content.

7. Performing the tests

7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.

7.3 The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.

7.4 The Buyer may raise and close Test Issues during the Test witnessing process.

7.5 The Supplier shall provide to the Buyer in relation to each Test:

7.5.1 a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and

7.5.2 the final Test Report within 5 Working Days of completion of Testing.

7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

7.6.1 an overview of the Testing conducted;

7.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;

7.6.3 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

7.6.4 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in

each case grouped by Severity Level in accordance with Paragraph 8.1; and

7.6.5 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

7.7 When the Supplier has completed a Milestone, it shall submit any Deliverables relating to that Milestone for Testing.

7.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.

7.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

8. Discovering Problems

8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.

8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

9. Test witnessing

9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and

requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

9.3 The Test Witnesses:

9.3.1 shall actively review the Test documentation;

9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

9.3.3 shall not be involved in the execution of any Test;

9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

9.4 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

10.Auditing the quality of the test

10.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

10.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

10.3 The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit.

10.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

10.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.

10.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction

Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

11. Outcome of the testing

11.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:

11.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;

11.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

11.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:

11.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

11.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.

11.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).

11.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.

11.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.

11.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer's report pursuant to Paragraph 10.5); and

11.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

12.Risk

12.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:

12.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or

12.1.2 affect the Buyer's right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

Annex 1: Test Issues – Severity Levels

1. Severity 1 Error

1.1 This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

2. Severity 2 Error

2.1 This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:

2.1.1 causes a Component to become unusable;

2.1.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

2.1.3 has an adverse impact on any other Component(s) or any other area of the Deliverables;

3. Severity 3 Error

3.1 This is an error which:

3.1.1 causes a Component to become unusable;

3.1.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

3.1.3 has an impact on any other Component(s) or any other area of the Deliverables;

but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

4. Severity 4 Error

4.1 This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

5. Severity 5 Error

5.1 This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

Annex 2: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

Dear Sirs,
Satisfaction Certificate
Deliverable/Milestone(s): [Insert relevant description of the agreed Deliverables/Milestones].

We refer to the agreement (**"Call-Off Contract"**) [insert Call-Off Contract reference number and any applicable SOW reference] relating to the provision of the [insert description of the Deliverables] between the [*insert Buyer name*] (**"Buyer"**) and [*insert Supplier name*] (**"Supplier"**) dated [*insert Call-Off Start Date dd/mm/yyyy*].

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]
[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].
Yours faithfully

[insert Name]

[insert Position]
acting on behalf of [insert name of Buyer]

Call-Off Schedule 14A (Service Levels)

1. Definitions

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

“Critical Service Level Failure”	has the meaning given to it in the Order Form;
"Service Credits"	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Order Form
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level
"Service Level Performance Measure	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2. What happens if you don’t meet the Service Levels

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier’s failure to meet any Service Level Performance Measure.

2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

(c) results in the corruption or loss of any Government Data; and/or

(d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and

2.5.3 there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits - NOT APPLICABLE

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

KPI/SLA	Service Area	KPI/SLA description	Target
1	Mobilisation	The lead time to onboard resources for implementation	100% of the resources onboarded within seven (5) working days from contract award
2	Quality	Deliverables completed on-time and the relevant standard issued under this contract	100% of the deliverables completed on time and meeting acceptance criteria

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

3.2.3 details of any Critical Service Level Failures;

3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

3.2.6 such other details as the Buyer may reasonably require from time to time.

3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

3.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

4. Satisfaction Surveys

4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Call-Off Schedule 15 (Call-Off Contract Management)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint 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 Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

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 Contract 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 Contract Manager

3.1 The Supplier's Contract Manager's 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 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 Contract Manager's responsibilities and obligations;
- 3.1.3 able to cancel any delegation and recommence the position himself; and
- 3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Managers in regards to the Contract and it will be the Supplier's Contract

Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager's 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 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 the Order Form.

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 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 Call-Off 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 Call-Off Contract which the Buyer's and the Supplier have identified.

Annex: Contract Boards

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

N/A

Call-Off Schedule 16 (Benchmarking)

1. DEFINITIONS

1.1In this Schedule, the following expressions shall have the following meanings:

"Benchmark Review" a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value;

"Benchmarked Deliverables" any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule;

"Comparable Rates" the Charges for Comparable Deliverables;

"Comparable Deliverables" deliverables that are identical or materially similar to the Benchmarked Deliverables (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar Deliverables exist in the market, the Supplier shall propose an approach for developing a comparable Deliverables benchmark;

"Comparison Group" a sample group of organisations providing Comparable Deliverables which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be fair comparators with the Supplier or which, are best practice organisations;

"Equivalent Data" data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group;

"Good Value" that the Benchmarked Rates are within the

Upper Quartile; and

"Upper Quartile" in respect of Benchmarked Rates, that based on an analysis of Equivalent Data,the Benchmarked Rates, as compared to the range of prices for Comparable Deliverables, are within the top 25% in terms of best value for money for the recipients of Comparable Deliverables.

2. **When you should use this Schedule**

2.1The Supplier acknowledges that the Buyer wishes to ensure that the Deliverables, represent value for money to the taxpayer throughout the Contract Period.

2.2This Schedule sets to ensure the Contracts represent value for money throughout and that the Buyer may terminate the Contract by issuing a Termination Notice to the Supplier if the Supplier refuses or fails to comply with its obligations as set out in Paragraphs 3 of this Schedule.

2.3Amounts payable under this Schedule shall not fall with the definition of a Cost.

3. Benchmarking
3.1**How benchmarking works**

3.1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.
3.1.2 The Buyer may, by written notice to the Supplier, require a Benchmark Review of any or all of the Deliverables.
3.1.3 The Buyer shall not be entitled to request a Benchmark Review during the first six (6) Month period from the Contract Commencement Date or at intervals of less than twelve (12) Months after any previous Benchmark Review.
3.1.4 The purpose of a Benchmark Review will be to establish whether the Benchmarked Deliverables are, individually and/or as a whole, Good Value.
3.1.5 The Deliverables that are to be the Benchmarked Deliverables will be identified by the Buyer in writing.
3.1.6 Upon its request for a Benchmark Review the Buyer shall nominate a benchmarker. The Supplier must approve the nomination within ten (10) Working Days unless the Supplier provides a reasonable explanation for rejecting the appointment. If the appointment is rejected then the Buyer may propose an alternative benchmarker. If the Parties cannot agree the appointment within twenty (20) days of the initial request for Benchmark review then a benchmarker shall be selected by the Chartered Institute of Financial Accountants.
3.1.7 The cost of a benchmarker shall be borne by the Buyer (provided that each Party shall bear its own internal costs of the Benchmark Review) except where the Benchmark Review demonstrates that the Benchmarked Service and/or the Benchmarked Deliverables are not Good Value, in which case the Parties shall share the cost of the benchmarker in such proportions as the Parties agree (acting reasonably). Invoices by the benchmarker shall be raised against the Supplier and the relevant portion shall be reimbursed by the Buyer.

3.2 Benchmarking Process

3.2.1 The benchmarker shall produce and send to the Buyer, for Approval, a draft plan for the Benchmark Review which must include:

(a) a proposed cost and timetable for the Benchmark Review;
(b) a description of the benchmarking methodology to be used which must demonstrate that the methodology to be used is capable of fulfilling the benchmarking purpose; and
(c) a description of how the benchmarker will scope and identify the Comparison Group.

3.2.2 The benchmarker, acting reasonably, shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking.
3.2.3 The Buyer must give notice in writing to the Supplier within

ten (10) Working Days after receiving the draft plan, advising the benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan.
3.2.4 Once both Parties have approved the draft plan then they will notify the benchmarker. No Party may unreasonably withhold or delay its Approval of the draft plan.
3.2.5 Once it has received the Approval of the draft plan, the benchmarker shall:

(a) finalise the Comparison Group and collect data relating to Comparable Rates. The selection of the Comparable Rates (both in terms of number and identity) shall be a matter for the Supplier's professional judgment using:
(i) market intelligence;
(ii) the benchmarker's own data and experience;
(iii) relevant published information; and
(iv) pursuant to Paragraph 3.2.6 below, information from other suppliers or purchasers on Comparable Rates;
(b) by applying the adjustment factors listed in Paragraph 3.2.7 and from an analysis of the Comparable Rates, derive the Equivalent Data;
(c) using the Equivalent Data, calculate the Upper Quartile;
(d) determine whether or not each Benchmarked Rate is, and/or the Benchmarked Rates as a whole are, Good Value.

3.2.6 The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the benchmarker in order to undertake the benchmarking. The Supplier agrees to use its reasonable endeavours to obtain information from other suppliers or purchasers on Comparable Rates.
3.2.7 In carrying out the benchmarking analysis the benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data:

(a) the contractual terms and business environment under which the Comparable Rates are being provided (including the scale and geographical spread of the customers);
(b) exchange rates;
(c) any other factors reasonably identified by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive.

3.3 Benchmarking Report

3.3.1 For the purposes of this Schedule "Benchmarking Report" shall mean the report produced by the benchmarker following the Benchmark Review and as further described in this Schedule;
3.3.2 The benchmarker shall prepare a Benchmarking Report and deliver it to the Buyer, at the time specified in the plan Approved pursuant to Paragraph 3.2.3, setting out its findings.

Those findings shall be required to:

(a) include a finding as to whether or not a Benchmarked Service and/or whether the Benchmarked Deliverables as a whole are, Good Value;

(b) if any of the Benchmarked Deliverables are, individually or as a whole, not Good Value, specify the changes that would be required to make that Benchmarked Service or the Benchmarked Deliverables as a whole Good Value; and

(c) include sufficient detail and transparency so that the Party requesting the Benchmarking can interpret and understand how the Supplier has calculated whether or not the Benchmarked Deliverables are, individually or as a whole,Good Value.

3.3.3 The Parties agree that any changes required to this Contract identified in the Benchmarking Report shall be implemented at the direction of the Buyer in accordance.

Call-Off Schedule 18 (Background Checks)

1. When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on the Contract.

2. Definitions

"Relevant Conviction" means any conviction listed in Annex 1 to this Schedule.

3. Relevant Convictions

3.1.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

3.1.2 Notwithstanding Paragraph 3.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

(a) carry out a check with the records held by the Department for Education (DfE);

(b) conduct thorough questioning regarding any Relevant Convictions; and

(c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

[Insert Relevant Convictions here]

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out as Attachment 3 - Statement of Requirements, the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

Attachment 3 – Statement of Requirements

Contract Reference: **P11407**

Infected Blood Compensation Authority
IBSS Discovery workpackage

CONTENTS

1. PURPOSE 144
2. BACKGROUND TO THE Buyer 144
3. Background to requirement/OVERVIEW of requirement 145
4 DEFINITIONS 145
5 Scope of requirement 146
6. The requirement 146
7. key milestones and Deliverables 150
8. Buyer Responsibility 151
9. Management Information/reporting 151
10. volumes 151
11. continuous improvement 151
12. Sustainability / SOCIAL VALUE 152
13. quality 152
14. PRICE 152
15. STAFF AND CUSTOMER SERVICE 152
16. service levels and performance 152
17. Security and CONFIDENTIALITY requirements 153
18. payment AND INVOICING 153
19. CONTRACT MANAGEMENT 153
20. Location 154

1. PURPOSE

1.1 The Infected Blood Compensation Authority (IBCA) requires a contract in place for the provision of digital specialist professional services to undertake a discovery into the transfer of Infected Blood Support Schemes (IBSS) into the Infected Blood Compensation Authority.

2. BACKGROUND TO THE BUYER

2.1 *Cabinet Office*

The Cabinet Office (CO) is the department that assists and ensures the effective running of Government. The Cabinet Office is also the corporate headquarters for the Government, in partnership with HM Treasury, and takes the lead in certain critical policy areas. In 2017, HMG commissioned the Infected Blood Inquiry - an independent inquiry, chaired by Sir Brian Langstaff - with a view of giving long awaited recognition, answers and a voice to the infected blood community. Following the inquiry's conclusion in May 2024, the Cabinet Office, as sponsor department for the inquiry over the past 6 years, has taken responsibility for establishing a new Non Departmental Public Body (NDPB), which will administer compensation payments to eligible members of the infected blood community. The CO will serve as the sponsor department for IBCA.

2.2 Infected Blood Compensation Authority (IBCA)

The Infected Blood Compensation Authority (IBCA) has been established by the Cabinet Office to deliver the Infected Blood Compensation Scheme, providing financial compensation to eligible people in the infected blood community. In a unique context of high political pressure, the CO must strike a fine balance between:

- Delivering at unprecedented pace to establish a large-scale Non-Departmental Public Body (NDPB) and continuing to pay compensation
- Addressing complex service requirements, whilst demonstrating value for money.
- Meeting the needs of vulnerable users

In the c.11 months since its inception, Infected Blood Compensation Authority (IBCA) has made massive progress towards its objective to stand up a fully operational Non-Departmental Public Body (NDPB).

IBCA made the first compensation payments to people in the infected blood community in 2024, and continues to make payments as well as developing its capability as a service focussed organisation.

The IBCA Digital team is working to develop and build a scalable service and we now seek continued support to advance work on understanding what will be needed to effectively transfer the existing Infected Blood Support Schemes into IBCA.

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 The UK government put in place Infected Blood Support Schemes (IBSS) for those who have been historically infected with Hepatitis C and/or HIV from NHS blood or blood products, as well as their spouses, civil or long-term co-habiting partners following the death of someone infected who was already a member of a current or former scheme.

3.2 There are four schemes, representing each of the constituent nations of the United Kingdom - Wales, Scotland, Northern Ireland and England.

3.3 The support schemes make payments and provide support to those who contracted hepatitis C and/or HIV via NHS blood transfusions or blood products before September 1991.

3.4 The four schemes are to be transitioned to the Infected Blood Compensation Authority (IBCA) by 31 March 2026.

3.5 The Supplier shall undertake a Discovery to develop and document a comprehensive understanding of the existing processes and identify and validate user needs and requirements to be met in transitioning the IBSS schemes to IBCA.

3.6 The approach and output of the discovery must be in line with the GDS digital service standard.

4 DEFINITIONS

Expression or Acronym	Definition
Authority	means the Contracting Authority. In this case, the Cabinet Office
Parties	means the Contracting Authority and the Supplier
IBCA	means Infected Blood Compensation Authority

IBSS	means Infected Blood Support Scheme(s) - there are four schemes, one for each of the constituent nations of the United Kingdom - Wales, Scotland, Northern Ireland and England

5 SCOPE OF REQUIREMENT

5.1 The Cabinet Office, on behalf of the Infected Blood Compensation Authority (IBCA), is seeking to appoint a suitably qualified specialist professional service provider (Supplier) to support the delivery of the Infected Blood Compensation Service in a way which is user centred, fast paced and scalable. In doing so, the appointed Supplier will support IBCA to understand the long term requirements of the service.

5.2 The Supplier shall produce a discovery report outlining the requirements and needs for the transfer of the IBSS schemes to IBCA. This will comprise, but not limited to the following key areas:

5.2.1 A detailed exploration of the IBSS schemes as organisations, including their responsibilities, obligations, and operational frameworks.

5.2.2 Analysing and mapping the current context in terms of existing roles, current processes, data currently available and technology in use.

5.2.3 Conduct user research to gather insights from stakeholders, identifying specific needs and experiences related to IBSS schemes.

5.2.4 Comprehensive documentation will include:

5.2.4.1 A detailed scope of onboarding the IBSS schemes, highlighting specific user needs and requirements.

5.2.4.2 Summaries of all analysis and user research conducted throughout the Discovery Phase, as well as the supporting data, interview scripts and other working documentation.

5.2.4.3 A gap analysis of the IBSS capabilities and processes of IBCA's, and what develop work would be required to enable a smooth transfer.

5.2.4.4 Recommendations outlining the next steps required for a smooth transition to IBCA.

5.2.4.5 A thorough Stakeholder analysis to ensure all relevant parties are considered

5.2.5 The Supplier will provide their own laptops and end user devices for the Discovery work.

6. THE REQUIREMENT

6.1 ***Functional Requirements***

In addition to those outlined in section 5 of this document, the Supplier will need to meet the following overarching requirements.

6.2 The Supplier will provide a Discovery Report before the end of the Contract. The Discovery Report is expected to be a standalone document that brings together all findings.

6.3 The Supplier will present learnings to the Authority twice weekly throughout the Discovery period, and propose next steps as part of the Discovery .

6.4 Discovery work will be carried out in accordance with the GDS Service Standard.

6.5 The Authority and Supplier will run a Discovery Kick-off meeting to give a summary of the current understanding of the problem area, share key contacts, specific standards and artefacts.

6.6 The Authority will provide a point of contact for questions throughout the Discovery period.

6.7 TUPE does not apply in this contract

Capability

IBCA will require the following skills sets:

- User research
- Business analysis
- Agile delivery management
- Product management

This Supplier will be able to provide capabilities detailed above and aligned to the definition of the role and skill sets set out in the current and future iterations of the Digital, Data and Technology (DDaT) roles in government and the skills needed to do them as described here:

https://ddat-capability-framework.service.gov.uk/

The Supplier will be able to provide capabilities listed above across SFIA grades 4-6 inclusive as described in the current and future iterations SFIA framework.

https://sfia-online.org/en/sfia-8/responsibilities

Quality

The Supplier will be able to ensure the delivery of quality outputs in accordance with the Cabinet Office Quality Process/Strategy as well as supporting the Buyer in enhancing and improving the process and its implementation across the services.

The Buyer will review the Deliverables against the Acceptance Criteria and the Performance Criteria as defined in sections 7 and 15 respectively. The Supplier must:

1. Ensure that Deliverables and any Services provided comply with the Buyer's requirements, and take into account feedback from check-in meetings.
2. Ensure that any Deliverables are produced in accordance with the Quality Plans to ensure they are of sufficient quality and standard to meet the Acceptance Criteria.
3. Manage and escalate risks and issues as appropriate, in accordance with the provisions of the Contract.
4. Conduct user research to the GDS Service Standard.
5. Have a research quality assurance policy in place that aligns with an external standard such as the Market Research Society Code of Conduct, the UK Research Integrity Office Code of Practice or other suitable recognised standard.

Delivery

The Supplier must deliver against the milestones and key performance indicators (KPIs) outlined in sections 7 and 15 respectively

The Supplier must attend relevant governance meetings.

The Supplier shall use their own assets (equipment/hardware) to fulfill the Buyer Requirements.

Behaviours

The Supplier must be able to commence delivery of the Services within 5 working days after this contract has been jointly signed by the Parties

The Supplier must adhere to the Buyer's Code of Conduct.

The Supplier must work in a collaborative manner, including with other third party Suppliers to the Buyer and the Buyer's staff at all organisational levels.

The Supplier must be able to demonstrate proactivity in sharing knowledge and experiences with members of the Buyer's staff.

The Supplier must be able to promote ideas and provide open suggestions as applicable, demonstrating innovative ideas and value-added initiatives as part of the contract management process.

Data Protection

The Supplier shall comply with the provisions of the Contract regarding Data Protection namely Annex 1 - Processing Personal Data of the Joint Schedule 11 (Processing Data).

The Supplier shall ensure any obligations on Key Sub Contractors or SubContractors as outlined in the Contract are adhered to.

All data and provision of services shall be held in the UK unless agreed (in writing) otherwise by the Buyer.

The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Key Sub-contractors or Subcontractors) for the provision of the Services.

Mandatory Requirements

- **Cyber Essentials Plus accreditation**: the Supplier must hold and maintain Cyber Essential Plus certification.
- **ISO/IEC 27001:2022 certifications** by a UKAS- recognised Certification Body
- **Cabinet Office Security Management Requirements**: the Supplier shall adhere to the Security Management Requirements during the period of the Contract as per Annex 1.
- **Vetting Requirements:** the Supplier undertakes that all Supplier Personnel will hold Baseline Personnel Security Standard (BPSS). The Supplier will evidence clearance of all staff deployed to IBCA work within the contract's first week.
- **Conflicts of interest:** The Supplier shall complete the Conflict of Interest form as provided in Annex 2 and notify the Cabinet Office any potential, actual or perceived conflicts of interest.
- **Safeguarding**

  1. The parties acknowledge that the Supplier is responsible for the management and control of the activity provided under this Work Order and for the purposes of the Safeguarding Vulnerable Groups Act 2006. The Supplier shall act in accordance with any relevant statutory framework, legislation, policy or guidance.

  2. The Supplier shall comply with the Buyer's safeguarding policies as amended from time to time.

  3. The Supplier shall comply with all statutory obligations including but not

limited to safeguarding and any relevant statutory obligations relating to the delivery of the Specialist Professional Services.

7. KEY MILESTONES AND DELIVERABLES

7.1 The start and end dates below are provided as guidance and will be formalised and agreed prior to contract award.

Milestone Reference	Deliverables	Description	Due Date
1	a)Supplier stand up Discovery team	• Supplier stand up Discovery team, and kick-off event held with Authority	Within 5 working days of signature
	b)Regular Discovery check-ins	• Supplier meet with Authority to play back learnings and share plan for next steps	Twice weekly throughout Discovery period
	c)Completion of Discovery Report	• A detailed scope of onboarding the IBSS schemes, highlighting specific user needs and requirements • Documented user and business needs with supporting evidence • Collated business analysis and user research conducted throughout the Discovery Phase • Recommendations outlining the next steps required for a smooth transition to IBCA • A thorough Stakeholder analysis to ensure all relevant parties are considered • Each of these is presented to the IBCA team for sign-off and handed over in full	Within 20 working days of start of Discovery period

8. Buyer Responsibility

8.1 The Buyer shall provide the Supplier an initial overview, outline documents and key contacts to enable completion of the task detailed in the Section 5 and 6.

8.2 The Buyer shall provide key contacts and introductions to enable the effective business analysis gathering and understanding of user needs for the Discovery work. These people must be available to support the activities in line with the agreed plan.

8.3 The Buyer shall provide responses to the Supplier's questions within 1 working day wherever reasonably possible.

8.4 The Buyer shall provide feedback and/or approval to the Supplier's documentation or deliverable within 2 working days.

9. Management Information/reporting

9.1 The Supplier will provide a lightweight weekly progress report on the delivery of the Milestones/Deliverables including:

1.1.1 RAG status of the delivery, and path to Green where delivery is reported as Red or Amber

1.1.2 The work committed to for the week and what has/has not been completed (and for those not an explanation as to why).

1.1.3 The work committed for the next week.

1.1.4 Risks, issues and/or dependencies.

10. volumes

10.1 N/A – resource based, not software.

11. continuous improvement

11.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

11.2 The Supplier should present new ways of working to the Buyer during weekly Contract review meetings.

11.3 The Supplier shall present learnings so far to the Buyer as part of a twice-weekly Discovery Review meeting.

11.4 Changes to the way in which the Services are to be delivered must be brought to the Buyer's attention and agreed prior to any changes being implemented.

12. SUSTAINABILITY / SOCIAL VALUE

12.1 The Supplier should include how it will commit to achieving Social Value Outcome:' Commitment to support health and well being, including physical and mental'

The latest guidance can be found here.

Details of the Social Value Model can be found here

13. QUALITY

13.1 All Supplier outputs are to be delivered as per GDS standards and signed off by the IBCA Interim Director of Digital.

13.2 The Supplier is expected to provide resources that will ensure the ongoing delivery of the IBCA Digital Service.

14. PRICE

14.1 The applicable Pricing Mechanism for this Contract is Milestone Payments on a Firm Price basis,

Bidder shall provide day rates for the DDaT roles listed within this SOR and for SFIA grades as part of the bid.

14.2 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

15. STAFF AND CUSTOMER SERVICE

15.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

15.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

15.3 The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.

16. SERVICE LEVELS AND PERFORMANCE

16.1 The Buyer will measure the quality of the Supplier's delivery by:

KPI/SLA	Service Area	KPI/SLA description	Target
1	Mobilisation	The lead time to onboard resources for implementation	100% of the resources onboarded within seven (5)

			working days from contract award
2	Quality	Deliverables completed on-time and the relevant standard issued under this contract	100% of the deliverables completed on time and meeting acceptance criteria

17. SECURITY AND CONFIDENTIALITY REQUIREMENTS

17.1 The Supplier shall comply with the Security clauses in this Contract, including but not limited to those contained within Information Security Management which can be found in Annex 1

17.2 The Supplier implementation resource must be cleared to BPSS level. The Supplier will evidence clearance of all staff deployed to IBCA within the contract's first week.

17.3 All work must be completed within the UK, offshoring of any work will not be permitted.

17.4 The Supplier must not take any live data from an IBCA system into theirs

17.5 The Supplier should be ISO/IEC 27001 certified.

18. PAYMENT AND INVOICING

18.1 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

18.2 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

18.3 Invoices should be submitted to:**REDACTED TEXT under FOIA Section 40, Personal Information**

18.4 Any invoices should be accompanied with the agreement of the IBCA Interim Director of Digital.

19. CONTRACT MANAGEMENT

19.1 The contract will be managed by IBCA's Interim Director of Digital, who will require the following:

- Weekly reports setting out progress against key milestones and targets.

- Weekly meetings (personnel to be agreed) to review weekly reports and progress.
- Ad hoc meetings and responses to queries which the Contract Manager has on a daily basis.

19.2 Should there be significant issues in delivering against these milestones, the CO and the Supplier will work together to manage them efficiently and effectively. If required, a performance improvement plan will be agreed with the Supplier, to get the project back on track. Any additional hours that are required as a result of this improvement plan will be delivered within the price agreed.

In addition, the contract management meetings may increase in regularity during the implementation of any improvement plan - attendance by the Supplier at these more regular contract management meetings will be required.

19.3 Attendance at Contract Review meetings shall be at the Supplier's own expense.

20. Location

20.1 The Service shall be delivered remotely.

20.2 The Supplier may be required to attend meetings/workshop to the 4 IBSS locations:
REDACTED TEXT under FOIA Section 40, Personal Information

20.3 The on-site location of the IBCA digital team is **REDACTED TEXT under FOIA Section 40, Personal Information**.