Crown Commercial Service

G-Cloud 11 Call-Off Contract (version 4)

Contents

Part A - Order Form

Digital Marketplace service ID number:	796537013139615
Call-Off Contract reference:	CCSO20A95
Call-Off Contract title:	Provision of replacement Case Management System (CMS)
Call-Off Contract description:	To provide the contracting authority with the replacement of case management system
Start date:	25 November 2020
Expiry date:	24 November 2022
Call-Off Contract value:	£200,567.00 excluding VAT
Charging method:	Invoicing amounts shall be in line with the Call-Off Charges at Schedule 2; subscription items shall be invoiced quarterly in advance, training items and onboarding services items to be invoiced at the beginning of the month following the month in which those items were delivered. The first period to which the subscription fee will apply will be the ten months from 25th January 2021 to 24th November 2021. An initial invoice will be raised to cover the period from 25th January 2021 to 24th February 2021. Thereafter, invoices will be raised quarterly in advance.
Purchase order number:	To be confirmed by the Buyer upon Contract Award

This Order Form is issued under the G-Cloud 11 Framework Agreement (RM1557.11).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From: The Buyer	HMT REDACTED
To: The Supplier	Civica UK LTD REDACTED
Together: the 'Parties'	

Principal contact details

For the Buyer:	REDACTED
For the Supplier:	REDACTED

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 25th November 2020 and shall operate until 24th of November 2022
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for 2 period(s) of 12 months each, by giving the Supplier 3 months written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. [The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each.

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot:	This Call-Off Contract is for the provision of Services under:

	Lot 2 - Cloud software.
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:

	• The service must include provisioning and support of the CMS. • The service must be for a cloud-based CMS. • The service must include the migration of data and documents from the incumbent supplier to a new supplier. • The service must support a minimum of 50 OFSI users (who may all be concurrent users). • The service must also support a minimum of 10 TLA (Treasury Legal Advisors) who require read only access. • The solution must be highly configurable to meet the authority requirements • The solution will be based on COTS software. • The service must include a full audit history. • Access to data and functionality must depend on user category and team. • The system must be capable of supporting the department with managing information in accordance with HMT's data retention policy. • The system must be straightforward to modify the system as the work of OFSI evolves. • The system will optionally have a full integration with the OFSI Consolidated List application hosted in Microsoft Azure which holds data on designated persons and regimes. • The system will integrate with Office 365 so that all documents and emails can be opened saved or sent from within the system. • The system will support all widely used document and file formats. • The system will support the use of generic email OFSI email addresses for inbound and outbound emails rather than users personal email addresses. • The system will have the ability to effectively manage Freedom of Information (FOI) requests. • The system must be monitored to ensure optimum performance. • The offering must include full archive, backup and disaster recovery provision.
Additional Services:	Not applicable
Location:	The Services will be delivered to 1 Horse Guards Road, London, SW1A 2HQ

<table>
<tr><td></td><td></td></tr>
<tr><td>Quality standards:</td><td>The quality standards required for this Call-Off Contract are as the Service Listing and as per Schedule 8 – Statement of Requirements.

The system must have the ability to access or export data which can be used for a range of management reporting, such as KPI information.

The system must provide the functionality to download data in a range of formats based on user reporting needs.</td></tr>
<tr><td>Technical standards:</td><td>The technical standards required for this Call-Off Contract are as per the Service Listing and as per Schedule 8 – Statement of Requirements.

It is expected that the bidder will operate to a recognised industry methodology and related delivery standards in order to structure and manage the project, for example, the use of Prince2, compliance with ISO9001</td></tr>
<tr><td>Service level agreement:</td><td>The Support service level agreement is as per the G-Cloud Service ID’s page and Service Definition document for the “Standard” offering. The Specific Service levels required for this contract are as below and have been confirmed by the Supplier to be within their G-Cloud Service Offering.

<table>
<tr><th>KPI/SLA</th><th>Service Area</th><th>KPI/SLA description</th><th>Target</th></tr>
<tr><td>1</td><td>Availability</td><td>The System must be available 24/7, except for periods of scheduled maintenance and planned downtime</td><td>99%</td></tr>
<tr><td>2</td><td>Critical Issues</td><td>For the highest level of prioritised issues (critical), for example when the service is not available at all, the resolution target must be within two hours.</td><td>95%</td></tr>
<tr><td>3</td><td>Critical Issues</td><td>It must be possible to report critical issues on a 24/7 basis</td><td>100%</td></tr>
<tr><td>4</td><td>Maintenance</td><td>Scheduled maintenance must only take place outside of the agreed core hours (which must be at least 9am to 5:30pm Mon-Fri excluding public holidays)</td><td>100%</td></tr>
<tr><td>5</td><td>Service reporting</td><td>Reporting for service issues is to be provided at quarterly intervals</td><td>95%</td></tr>
</table>
</td></tr>
</table>

Onboarding:	Implementation and training services form part of the project deliverables agreed under this Contract.
Offboarding:	Under Clause 21.2 an Exit Plan is required to be completed. This shall be submitted and agreed with the Buyer by no later than three (3) months from Contract Commencement. The offboarding plan for this Call-Off Contract will be in line with the Exit Plan created in accordance with Clause 21 'Exit Plan' and Clause 22 'Handover to replacement Supplier' of the Call-Off Terms and Conditions.
Collaboration agreement:	Not applicable
Limit on Parties' liability:	The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for all other defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance:	The insurance(s) required will be: • Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • Employers; liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 10 consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: Framework audit provision clause 7.4 to 7.13 as and when required in agreement between the Buyer and the Supplier.
Buyer's responsibilities:	The Buyer is responsible for ensuring the Supplier has the Buyer held information required in order to ensure successful delivery of the Contract.
Buyer's equipment:	The Buyer's equipment to be used with this Call-Off Contract includes: In the event of a scenario where the Buyer's equipment is required then this will be by written agreement between the Buyer and Supplier only. Written agreement must confirm what equipment, limitations of the use, any policies which must be followed and duration of use permitted.

Supplier's information

Subcontractors or partners:	Not applicable

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method:	The payment method for this Call-Off Contract is via BACS
Payment profile:	The payment profile for this Call-Off Contract is as per the Charging Method, repeated below: Invoicing amounts shall be in line with the Call- Off Charges at Schedule 2; subscription items shall be invoiced quarterly in advance, training items and onboarding services items to be invoiced at the beginning of the month following the month in which those items were delivered. The first period to which the subscription fee will apply will be the ten months from 25th January 2021 to 24th November 2021. An initial invoice will be raised to cover the period from 25th January 2021 to 24th February 2021. Thereafter, invoices will be raised quarterly in advance.
Invoice details:	The Supplier will issue electronic invoices. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice
Who and where to send invoices to:	REDACTED
Invoice information required – for example purchase order, project reference:	All invoices must include: A valid purchase order number Detailed and complete breakdown of all Charges incurred.
Invoice frequency:	Invoice will be sent to the Buyer in line with the payment profile set forth above.
Call-Off Contract value:	The total value of this Call-Off Contract is £200,567.00 excluding VAT.
Call-Off Contract charges:	The breakdown of the Charges is in line with the payment profile set forth above. The breakdown of the Charges is as detailed within Schedule 2 – Call off Charges

Additional Buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following implementation plan, exit and offboarding plans and milestones:

Milestone/Deliverable	Description	Timeframe or Delivery Date

	1	Completion of application configuration, phased UAT and migration test	No later than 31/01/2021
	2	Completion of end-to-end User Acceptance Testing and validation of the migration test	No later than 28/02/2021
	3	Completion of training and final migration and Go live	No later than 31/03/2021

Guarantee:	Not applicable
Warranties, representations:	Not applicable
Supplemental requirements in addition to the Call-Off terms:	Not applicable
Alternative clauses:	Not applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms:	Not applicable
Public Services Network (PSN):	Not applicable
Personal Data and Data Subjects:	Confirm whether either Annex 1 or Annex 2 of Schedule 7 is being used: Annex 1 / Annex 2 to be completed upon contract award.

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name:	REDACTED	REDACTED
Title:	REDACTED	REDACTED
Signature:	REDACTED	REDACTED
Date:	REDACTED	REDACTED

Schedule 1 - Services

The full Services required and details can be found within Schedule 8 – Statement of Requirements. The services required may be called off or required at any point and will be on agreement between both the Buyer and the Supplier.

Schedule 2 - Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

REDACTED

All Charges are excluding VAT. Any additional services required will be based upon the G-Cloud Service Listings applicable pricing document and only upon agreement between the Buyer and Supplier at the use of any additional services require

Part B - Terms and conditions

1. Call-Off Contract start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

- a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’
- a reference to ‘CCS’ will be a reference to ‘the Buyer’
- a reference to the ‘Parties’ and a ‘Party’ will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as ‘incorporated Framework clause XX’, where ‘XX’ is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier’s Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer’s acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier’s engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the

Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
- are confident that they can fulfil their obligations according to the Call-Off Contract terms
- have raised all due diligence questions before signing the Call-Off Contract
- have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of

the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer’s failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there’s an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn’t possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer’s volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

- a broker's verification of insurance
- receipts for the insurance premium
- evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any

insurances

- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

- premiums, which it will pay promptly
- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.78 to 8.86. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

- rights granted to the Buyer under this Call-Off Contract

- Supplier’s performance of the Services
- use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

- modify the relevant part of the Services without reducing its functionality or performance
- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.7 Clause 11.5 will not apply if the IPR Claim is from:

- the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract
- other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

- comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data
- only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
- take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions
- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

- providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

The Supplier must not remove any proprietary notices in the Buyer Data.

13.1 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policy and all Buyer requirements in the Order Form.

13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/collection/risk-management-collection
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6 The Buyer will specify any security requirements for this project in the Order Form.

13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

- Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start Date:

- an executed Guarantee in the form at Schedule 5
- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- an Insolvency Event of the other Party happens
- the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in

the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)
- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions

to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

Manner of delivery	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off

Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which is reasonably required to ensure continuity

of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
- other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from

breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start Date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status

- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

- its failure to comply with the provisions of this clause
- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn’t have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start Date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

- work proactively and in good faith with each of the Buyer's contractors
- co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.57 and 8.58 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.57 and 8.58 are reproduced in this Call-Off Contract document at schedule 7

Schedule 3 - Collaboration agreement

Not applicable

Schedule 4 - Alternative clauses

Not applicable

Schedule 5 – Guarantee

Not applicable

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.

Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; iii) (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this

	Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14-digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.11 together with the Framework Schedules.

Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-

	How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.

Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.

Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security Management Plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms

	and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: REDACTED
1.2 The contact details of the Supplier's Data Protection Officer are: REDACTED
1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: ● **The** Personal Data is collected for the purpose of meeting the obligation for implementing and enforcing financial sanctions. Data is stored and used by OFSI staff as detailed in the scope of requirements section 5 and the requirements section 6. This includes data on individuals subject to financial sanctions, members of the public, persons at external organisations, other government departments and user staff. OFSI also will process personal data collected for the purposes described above. In addition, the supplier and Amazon Web Services will process personal data provided in relation to the scope of requirements section 5 and the requirements in section 6.

Duration of the Processing	The duration of the contract.
Nature and purposes of the Processing	OFSI processes personal data in the course of its mission to help ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom. OFSI is structured in branches, each of which processes personal data for the execution of its core purposes as set out below: - **The Operations and Governance branch** leads on OFSI's day to day operations, and provides operational support across OFSI, overseeing corporate knowledge and data protection management, management of the OFSI Consolidated List (and associated notices) and Frozen Asset reporting. It also works closely with HMT centre on corporate returns; - **The International Engagement branch** helps promote robust financial sanctions implementation on the world stage, not only through the bilateral and multilateral meetings/events but also through technical assistance to other governments. - **The Litigation branch** is responsible for OFSI's litigation strategy and associated legal and financial risks, reporting on OFSI's legal costs and represents OFSI as a witness in Civil cases. It is responsible for recording, managing and responding to legal challenges. - **The Licensing branch** is responsible for making licensing decisions involving sanctioned persons/entities and working with Whitehall partners to influence Government policy on international sanctions, and. - **The Counter-Terrorism branch** implements the Terrorist Asset Freezing etc. Act 2010 which gives HMT powers to freeze the assets of those believed to be involved in terrorism, as well as implementing the EU's terrorist asset freezing regime and UN asset freezes. - **The Compliance branch** ensures that suspected breaches of financial sanctions are identified and investigated and where required recommends enforcement action. The branch also looks at whether to impose monetary penalties. - **The Guidance and Engagement branch** is responsible for raising awareness of financial sanctions and OFSI; promoting the

	importance of compliance to the private, public and not-for-profit sectors; and communicating the services OFSI provides - **The Operational Policy and Priority Projects branch** leads on operational policy development and implementation together with working on high-priority projects.
Type of Personal Data	Names, email addresses, location, biographical information, telephone numbers, official documentation (e.g. passport or NI numbers), financial information, criminal convictions information, and health information.
Categories of Data Subject	Individuals subject to financial sanctions, members of the public, HMT staff, and representatives of external organisations and other government departments
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	At the end of the Contract, in accordance with the Exit Plan, the Processor will support the Controller in the extraction of the Controller's data that is then current within the system. Upon confirmation by the Controller that such data extract has been successful, the Processor will delete all data from its systems.

Schedule 8 – Statement of Requirements

1. PURPOSE

1.1 HM Treasury has a requirement to provide the Office of Financial Sanctions Implementation (OFSI) with a replacement Case Management System (CMS) which will meet current and future business needs. OFSI helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Authority is the government's economic and finance ministry, maintaining control over public spending, setting the direction of the UK's economic policy and working to achieve strong and sustainable economic growth. HM Treasury's vision is to:

2.1.1 Reduce the structural deficit in a fair and responsible way; I.e. take action to tackle the deficit in a fair and responsible way, ensure that taxpayers' money is spent responsibly, and get the public finances back on track whilst protecting growth.

2.1.2 Secure an economy that is more resilient, and more balanced between public and private sectors and between regions; I.e. take action to boost enterprise, support green growth and build a fairer and more balanced economy where we achieve a sustainable distribution of growth across the economy, in particular within regions and sectors.

2.1.3 Reform the regulatory framework for the financial sector to avoid future financial crises; The current system of financial regulation is replaced with a framework that promotes responsible and sustainable banking, where regulators have greater powers to curb unsustainable lending practices and we take action to promote more competition in the banking sector.

2.2 HM Treasury is supported by a shared service function to fulfil all its ICT requirements. The ICT services are provided by the Information and Workplace Solutions (IWS) Team in conjunction with the Authority's outsourced providers.

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 The Office of Financial Sanctions Implementation (OFSI) helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom. OFSI, which is a part of HM Treasury, enables financial sanctions to make the fullest possible contribution to the UK's foreign policy and national security goals. It also helps to maintain the integrity of, and confidence, in the UK financial services sector.

3.2 The existing OFSI Case Management System (CMS) was developed as a bespoke application in 2016/17 and went into full live operation in March 2017. Whilst the CMS still supports their requirements, some compromises are having to be made in the way it is used. In addition, for technical and cost reasons, a number of features were deemed out of scope in the original project. It is therefore advisable to revisit the business's existing and future requirements and identify options which may provide benefits over the existing solution.

3.3 There are a growing number of pressure points on the current model, the team and its functions have expanded since 2016 and the sanctions landscape is ever-changing. Furthermore, the contract for the data centre currently in use for the CMS expires in 2022 and in addition Microsoft support for the version of SharePoint it uses (SP2013) will end in 2023.

4. DEFINITIONS

Expression or Acronym	Definition
CMS	Case Management System
COTS	Commercial off-the-shelf
FOI	Freedom of Information
HMT or HM Treasury	Her Majesty's Treasury
IWS	Information Workplace Solutions
OFSI	Office of Financial Sanctions Implementation
UAT	User Acceptance Testing

5. SCOPE OF REQUIREMENT

5.1 The service must include provisioning and support of the CMS.

5.2 The service must be for a cloud-based CMS.

5.3 The service must include the migration of data and documents from the incumbent supplier to a new supplier.

5.4 The service must support a minimum of 50 OFSI users (who may all be concurrent users).

5.5 The service must also support a minimum of 10 TLA (Treasury Legal Advisors) who require read only access.

5.6 The solution must be highly configurable to meet the authority requirements

5.7 The solution will be based on COTS software.

5.8 The service must include a full audit history.

5.9 Access to data and functionality must depend on user category and team.

5.10 The system must be capable of supporting the department with managing information in accordance with HMT's data retention policy.

5.11 It must be straightforward to modify the system as the work of OFSI evolves.

5.12 The system will optionally have a full integration with the OFSI Consolidated List application hosted in Microsoft Azure which holds data on designated persons and regimes.

5.13 The system will integrate with Office 365 so that all documents and emails can be opened saved or sent from within the system.

5.14 The system will support all widely used document and file formats.

5.15 The system will support the use of generic email OFSI email addresses for inbound and outbound emails rather than users personal email addresses.

5.16 The system will have the ability to effectively manage Freedom of Information (FOI) requests.

5.17 Any member of Supplier staff with access to production data, including production data in a test environment must have SC security clearance.

5.18 The system must be monitored to ensure optimum performance.

5.19 The offering must include full archive, backup and disaster recovery provision.

5.20 Administrator guides and technical manuals such as Application Programming Interface (API) documentation must be provided.

6. THE REQUIREMENT

6.1 Management of Regimes and Designated Persons:

6.1.1 The system will enable users to create a new designated person (a designated person is an individual, entity or body, listed under UK legislation as being subject to financial sanctions) based on data held in the OFSI consolidated list application.

6.1.2 The system will be able to clearly represent relationships between regimes, designated people and known aliases for a designated person.

6.1.3 Comprehensive information will be held about regimes.

6.2 Asset Recording

6.2.1 It will optionally be possible to record frozen assets of different types owned by a designated person and valued both in the local currency and GBP. Optionally, the system will be able to generate asset audit reports for example, a view of all frozen asset account balances for a designated person.

6.3 Recording Suspected Breach Reports

6.3.1 The system will be used to record monitor and update suspected breaches of a financial sanction, including the outcome of a suspected breach.

6.4 Licence Management

6.4.1 The system will be used to record and manage licences which have been granted to one or more designated persons to enable them to access assets. This will

include the licence application, the outcome and any subsequent amendments after issue.

6.4.2 Amendments to a licence will be available to view along with the associated documentation. Each amendment will have a distinct reference.

6.5 Management of Monetary Penalties

6.5.1 The system will manage the process of issuing monetary penalties against contacts or organisations who have breached a financial sanction and have met the legal requirement for a monetary penalty.

6.6 Association with Designated Persons and Contacts

6.6.1 In addition to recording the designated person and main contact for an asset, suspected breach, licence or monetary penalty it will be possible to associate other designated persons or contacts where necessary.

6.7 Litigation Management

6.7.1 The system must support any litigation between OFSI and designated persons, contacts or organisations by segregating the documents that relate to a specific litigation case.

6.8 Interaction Recording

6.8.1 The system will track and store all interactions with OFSI made by email, document or phone call and whether inbound or outbound against relevant contacts, organisations and designated person(s).

6.8.2 The interaction will be recorded against a breach, licence, monetary penalty or litigation if relevant.

6.9 References

6.9.1 The system will optionally allocate a unique visible reference to each interaction, breach, licence, monetary penalty or litigation.

6.10 Task Management

6.10.1 The system will be used to assign, reassign, prioritise, amend and track tasks at both individual and team level.

6.10.2 There will be a straightforward notification when tasks are created or modified and a simple method for tracking tasks for example, those which are close to their due date.

6.10.3 It will be straightforward to measure and report on the duration of tasks.

6.10.4 Tasks can be associated with one or more interactions, designated persons, contacts, organisations, breaches, licences, monetary penalties or litigation.

6.11 User Experience

6.11.1 The system must be able to present a consolidated view for a regime, designated person, organisation or contact. All relevant breaches, licences, financial penalties, litigation, tasks, interactions and documents will be shown with a timeline for context.

6.11.2 The system will be able to present a consolidated view of a task showing interactions, updates and a timeline.

6.11.3 Comprehensive search tools will be available allowing the user to quickly identify relevant information.

6.11.4 Each user will have a dashboard to assist them with managing their tasks or the tasks of their team.

6.12 Workflow management

6.12.1 The system will be able to generate tasks automatically and assign them to users.

6.13 General Reporting

6.13.1 The system will have the ability to search through the data it holds in order to identify information and artefacts relevant to a specific individual, Designated Person, organisation or regime.

6.13.2 The system will have the ability to create reports that include but is not limited to all the relevant data documents and interactions relating to a breach, licence monetary penalty, litigation, designated person, contact, organisation or task.

6.13.3 The system must support the production of sophisticated reports across multiple entities and provide the functionality for data visualisation or the export into other software packages for this purpose.

6.14 Templates and standard text

6.14.1 It will be possible to create documents based on templates and system data, for example, particular licences and emails.

6.15 Data De-duplication

6.15.1 Optionally, the system should provide data de-duplication tools.

6.16 Public Facing Forms

6.16.1 Online forms will be created which will have links to them from the GOV.UK domain and which will store data entered by external parties in the OFSI application.

6.17 User Support and administration

6.17.1 Service levels must be agreed and a table with response times for the authority's approval must be provided.

6.17.2 Support must be provided to ensure availability of the system and where incidents occur; the service provider needs to be highly responsive for high priority incidents.

6.17.3 The system must provide the ability to raise support tickets.

6.17.4 The system must incorporate a self-service option for frequent faults and issues.

6.17.5 The system must provide simple, powerful and flexible options for account management, including allowing the business to define the organisational hierarchy, roles & permissions.

6.17.6 Any changes made to the system must first be available for testing in a User Acceptance Test (UAT) environment. The Authority will give confirmation that UAT has been successfully completed prior to a release deployment into the Live environment.

6.18 Onboarding and data migration

6.18.1 Data cleansing must be performed prior to data migration.

6.18.2 Assistance with configuration and customisation required to ensure the CMS meets the requirements detailed in section 6.

6.18.3 All application data and documents from the current CMS are required to be moved from the incumbent to a new CMS.

6.18.4 Assistance must be provided with on-boarding users.

6.18.5 The system must support the ability to make configuration changes based on the Authority workflow and processes, and where possible a list of standard configuration change pricing is to be made available.

6.19 Training

6.19.1 Training must be tailored to the different roles using the system and will include the adaptations made to the system for OFSI.

6.19.2 Supporting documentation optionally should include the adaptations made to the system for OFSI.

6.20 Testing and Acceptance.

6.20.1 User acceptance testing to be completed to HMT's agreed standards with production quality data in an environment that mirrors production performance.

6.20.2 The UAT environment must interface to other test environments as appropriate to ensure successful end to end testing.

7. KEY MILESTONES AND DELIVERABLES

7.1 Our expectation is that the supplier delivers incrementally into a user acceptance test environment, e.g.:

7.1.1 A first delivery of across the board functionality used throughout the application (task creation, allocation, updating, etc.), followed by delivery of functional areas such as Licencing, Breaches, etc. These deliveries will be tested as a phased UAT using ad-hoc data.

7.1.2 When all functionality has been delivered then a migration test can be undertaken and an end to end UAT test made of the whole system with real data.

7.2 The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date
1	Completion of application configuration, phased UAT and migration test	No later than 31/01/2021
2	Completion of end-to-end User Acceptance Testing and validation of the migration test	No later than 28/02/2021
3	Completion of training and final migration and Go live	No later than 31/03/2021

8. MANAGEMENT INFORMATION/REPORTING

8.1 The system must have the ability to access or export data which can be used for a range of management reporting, such as KPI information.

8.2 The system must provide the functionality to download data in a range of formats based on user reporting needs.

9. VOLUMES

9.1 The service must be capable of handling annual volumes of:

- 100 Licence applications
- 100 Licence amendments
- 200 Designated Person additions
- 500 Consolidated List amendments
- 100 Breach Reports
- 1000 Tasks

10. CONTINUOUS IMPROVEMENT

10.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration, including sharing the product roadmap.

10.2 The supplier must be open to change suggestions from the Authority and provide continual development options

10.3 The Supplier must hold quarterly Contract review meetings with the Authority.

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

11. SUSTAINABILITY

11.1 There are no specific sustainability considerations relevant to the CMS requirement.

12. QUALITY

12.1 It is expected that the bidder will operate to a recognised industry methodology and related delivery standards in order to structure and manage the project, for example, the use of Prince2, compliance with ISO9001.

13. PRICE

13.1 Prices shall not exceed the Framework maximum rates.

14. STAFF AND CUSTOMER SERVICE

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

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

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

15. SERVICE LEVELS AND PERFORMANCE

15.1 The Authority will measure the quality of the Supplier's delivery by:

KPI/SLA	Service Area	KPI/SLA description	Target
1	Availability	The System must be available 24/7, except for periods of scheduled maintenance and planned downtime	99%
2	Critical Issues	For the highest level of prioritised issues (critical), for example when the service is not available at all, the resolution target must be within two hours.	95%
3	Critical Issues	It must be possible to report critical issues on a 24/7 basis	100%
4	Maintenance	Scheduled maintenance must only take place outside of the agreed core hours (which must be at least 9am to 5:30pm Mon-Fri excluding public holidays)	100%
5	Service reporting	Reporting for service issues is to be provided at quarterly intervals	95%

15.2 The supplier will operate a Service Credit system which will be applied if the annual availability of the system is less than the contractually agreed percentage. Circumstances outside of the Suppliers control (as agreed within the contract) will be factored into the calculation of annual availability.

15.3 In the event of early termination of the contract the Supplier must provide a complete copy of all data and documents held within the system in a format and timescale that is acceptable to HMT and which is agreed at the time of termination. Once this transfer has been validated by HMT the Supplier must ensure that their copies of the data and documents are deleted.

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

16.1 Suppliers must be able to fully support the Authority with the Government Security Policy Framework and that they have appropriate IT, physical, personnel and procedural security measures in place to prevent any unauthorised access to, or leakage of, data collected as part of this contract, and to prevent it being shared with any unauthorised third parties. Such security measures must comply with the requirements of the ISO 27001 standard as a minimum and the Authority would wish to see evidence of that compliance, e.g. in the form of current ISO 27001 certification.

16.2 Any IT systems used by Suppliers to meet the Authority's requirement must comply with National Cyber Security Centre (NCSC)'s 10 Steps to Cyber Security and with the NCSC's Cloud Security Principles**;**

16.3 Any IT systems that would be deployed by the Supplier to meet any part of the requirement must be subjected to periodic (at least annual) independent penetration testing carried out to NCSC CHECK terms and conditions, and any significant vulnerabilities identified as part of the penetration testing must be remediated with timeframes agreed with the Authority.

16.4 The Supplier must describe how, in order to ensure that reliance isn't placed solely on annual penetration testing to identify and address vulnerabilities, they might perform regular vulnerability scans on the component devices of the IT infrastructure and how they would ensure that any significant vulnerabilities identified by those scans are remediated as soon as possible.

16.5 Any IT systems that would be deployed by the Suppliers to meet any part of the requirements must enforce strict logical access management controls; it is mandatory that the Supplier can restrict access to only the Authorities public IP range. The Supplier solution will preferably also support Multi-Factor Authentication (MFA) and Single Sign-On (SSO) and have measures in place to prevent and audit Supplier system admin staff having access to Authority data.

16.6 Where any IT systems used by Suppliers to meet any part of the requirement need to generate any emails, the Supplier must be able to ensure that encryption and anti-spoofing measures can be applied to the emails which comply with the following guidance:

16.7 https://www.gov.uk/guidance/securing-government-email

16.8 Suppliers are expected to demonstrate they have appropriate physical security measures in place in any premises used to store/process the Authority's data. As above such physical security measures must comply with the requirements of ISO27001 as a minimum. Any data centres used by the Supplier to meet the Authority's requirement must hold current ISO27001 certification and are expected to be UK based. Where a Supplier may be proposing a solution that uses any non-UK based data centres that must be stated very clearly with an explanation of how all the stated Authority security requirements (including those in relation to personnel security and DPA 2018/GDPR compliance) can still be met.

16.9 Any pre-employment checks that the Supplier subjects their staff must be at least equivalent to the Government Baseline Personnel Security Standard. This would apply to the staff of any sub-contractors used by the Supplier to provide part of the service.

16.10 Any Supplier staff or sub-contractors (e.g. system administers and helpdesk support staff who would have access to Authority data) should either have or will be expected to undergo National Security Vetting to Security Check (SC) level.

16.11 Suppliers shall ensure that any suspected or actual security breaches related to Authority data/information are reported to the Authority immediately. Where any actual security breaches have been identified, Suppliers shall, as soon as reasonably practicable, provide to the Authority a report setting out the details of the security breach, including an impact assessment, a root cause analysis and the steps taken to address the breach.

16.12 Full compliance with the Data Protection Act (DPA) 2018 and the General Protection Regulation (GDPR) is essential.

16.13 Civica needs to provide Full Names and DoB of staff assigned to the project to send to HM Treasury's appointed security lead who will then be able to validate each person's current clearance status. [This would have to apply if additional members join the team as the project progresses].

16.14 Every 6 months the process needs to be repeated – i.e. for those Civica staff assigned to the ongoing service support.

17. PAYMENT AND INVOICING

17.1 Invoicing and payment will be under standard HMT terms and as per agreed invoicing milestones (To be agreed between the contracting authority at project initiation meeting).

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

17.3 Invoices should be submitted to: REDACTED

17.4 No invoice will be authorised without an associated purchase order number.

18. CONTRACT MANAGEMENT

18.1 Meetings will take place as agreed on a monthly or quarterly basis and shall be held at 1 Horse Guards Road providing that Covid-19 working arrangements permit this or otherwise via Microsoft Teams.

18.2 Attendance at Contract Review meetings shall be at the Supplier's own expense.

19. LOCATION

19.1 The location of the Services will be carried out at REDACTED