Crown Commercial Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	841180421436717
Call-Off Contract reference	710182450
Call-Off Contract title	Master Data Management
Call-Off Contract description	To analyse and document master data in the form of a master data catalogue which will provide a basis for all master data management activities and support new tasks aimed at rationalising and improving master data through data and process improvements. This will also set up a Canonical (Consolidated) Data Model across Defence Support that brings together and defines the standard set of data types, relationships and business rules that will help facilitate data exchange and interoperability.
Start date	This Call-Off contract starts on the date of last signature to this Call-Off Contract.
Expiry date	30-06-2024 If optional extension is invoked, the new contract expiry date will be confirmed by both parties but will not exceed 31/12/2024.
Call-Off Contract value	£ 821,632.00 excl. VAT
Charging method	CP&F Purchase Order
Purchase order number	[Enter purchase order number]

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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 Services 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 contact with square brackets.

From the Buyer	**REDACTED TEXT under FOIA Section 40, Personal Information** **REDACTED TEXT under FOIA Section 40, Personal Information** UKStratCom MOD Abbey Wood NH2 Larch 3B Mail point #2317 Bristol BS34 8JH
To the Supplier	Eviden Technology Services Limited Supplier's address: Supplier: Eviden Technology Services Limited Address: 44 Esplanade, St Helier Jersey, JE4 9WG Company Number: 146917 Acting through its UK Establishment: Supplier: Eviden Technology Services Limited Address: Second Floor, Mid City Place, London,71 High Holborn, WC1V 6EA Company Number: BR025381
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: **REDACTED TEXT under FOIA Section 43, Commercial Interests** Project Team

Name: **REDACTED TEXT under FOIA Section 40, Personal Information**

Email: **REDACTED TEXT under FOIA Section 40, Personal Information**

Phone: **REDACTED TEXT under FOIA Section 40, Personal Information**

For the Supplier:

Title: Mr
Name: **REDACTED TEXT under FOIA Section 40, Personal Information**
Email: **REDACTED TEXT under FOIA Section 40, Personal Information**
Phone: **REDACTED TEXT under FOIA Section 40, Personal Information**

Call-Off Contract term

Start date	This Call-Off Contract Starts on the date of last signature to the Call-Off Contract.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **30** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 6 months, by giving the Supplier **4 weeks** written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below. The enactment of the **Six** months extension period will first be subject to Authority approvals and discretion. Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

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 3: Cloud support
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: ● Master Data Catalogue ● Master Data Recommendations ● Canonical Data Model
Additional Services	**Added in Schedule 1- SOW**
Location	The Services will be delivered to Defence Support, Support Major Programmes, #3241

	Cedar 2A, NH3, MOD Abbey Wood, Bristol, BS34 8JH Will be working remotely
Quality Standards	The quality standards required for this Call-Off Contract are ISO27001
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are Digital Strategy - Digital Marketplace
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are mentioned in Schedule 1
Onboarding	N/A

Offboarding	N/A
Collaboration agreement	N/A

Limit on Parties' liability	Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed five hundred thousand pounds (£500,000) per year. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed five hundred thousand pounds (£500,000) per year**.** The annual total liability of the Supplier for all other Defaults will not exceed the value specified in Clause 24.1 of the Call Off Contract.
Insurance	The Supplier insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● 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 in the annual aggregate or any higher limit required by Law ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law

Buyer's responsibilities	Mentioned in Schedule 1- SOW
Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes: • MOD Laptops • MODnet Accounts Reason: To operate at Official sensitive and hold and store information on MOD systems as appropriate

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners N/A

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 the Contract, Purchasing & Finance system (CP&F), as is mandatory for all MoD payments as per DEFCON 522 (Edition 11/21) Payment and Recovery of Sums Due.
Payment profile	The payment profile for this Call-Off Contract is as follows: For Firm Price related Charges: Payment will be in accordance with Milestone Payment Plan detailed in the Call-Off Contract charges

	Payments may be subject to an overall 20.00% milestone retention against the full milestone value. See details in **Call Off Contract Charges**.
Invoice details	For Firm Price related Charges the Supplier will issue electronic invoices on achievement of the milestone via Exostar. A PDF copy of the invoice should be sent to the Commercial Officer for retention once the invoice has been submitted on Exostar. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice
Who and where to send invoices to	Invoices will be submitted to the Authority via Exostar on to CP&F. An electronic copy must also be sent to the buyer.
Invoice information required	All invoices must include the MOD provided contract reference number and the Purchase order no. The Purchase Order Number must include all information required by Exostar such as: ▪ The Supplier's name and address, ▪ The Purchase Order Number, ▪ The Project Reference, ▪ The date the invoice was submitted, ▪ The relevant year and dates the invoices relates to.
Invoice frequency	Invoice will be sent to the Buyer on successful submission of completed and approved deliverables and milestones.

Call-Off Contract value	The total value of this Call-Off Contract is **£ 821,632.00 excl. VAT**
Call-Off Contract charges	The proposed breakdown of the Charges are detailed in Schedule 2 Call Off Contract Charges

Additional Buyer terms

Performance of the Service	● The performance of the Service and Deliverables are measured in accordance with Schedule 1 (Services) to the Call Off Order and the accompanying Service Definitions to Schedule 1 (Services).
Guarantee	N/A
Warranties, representations	N/A

Supplemental requirements in addition to the Call-Off terms	Within the scope of the Call-Off Contract, the Supplier will ensure compliance with: DEFCONs 659a and 660 DEFCON 659A (Edition 09/21) – Security Measures DEFCON 660 (Edition 12/15) Official Sensitive Security “Further to DEFCON 658 the Cyber Risk Profile of the Contract is “N/A”, as defined in Def Stan 05-138.” Cyber Risk Assessment Reference Number RAR- 792277893 – Status Risk Level N/A **No further action from the Supplier.** DEFCON 005J (Edition 18/11/16) – Unique Identifiers DEFCON 129J (Edition 11/16) – The Use of the Electronic Business Delivery Form DEFCON 566 (Edition 10/20) – Change of Control of Contractor.
Alternative clauses	Not Applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms	Despite anything to the contrary elsewhere in the Call-Off Contract, the Buyer agrees that it will not publish the Supplier’s Background IPRs as open source. The Buyer will only provide information classified as up to and including Official-Sensitive without caveats, unless explicitly agreed with the Supplier in the writing and codified with a Security Aspects Letter.
Personal Data and Data Subjects	Annex 1 and Annex 2 of Schedule 7

Intellectual Property	As per clause 11
Social Value	Social Value As per the Social Value requirements in accordance with Schedule 1: Service

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 (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.

Signed	Supplier	Buyer
Name	**REDACTED TEXT under FOIA Section 40, Personal Information**	**REDACTED TEXT under FOIA Section 40, Personal Information**
Title	Client Executive Partner	Commercial Manager

Signature	**REDACTED TEXT under FOIA Section 40, Personal Information**	**REDACTED TEXT under FOIA Section 40, Personal Information**
Date	21/02/2024	21/02/2024

2.2 The Buyer provided an Order Form for Services to the Supplier.

Customer Benefits
For each Call-Off Contract please complete a customer benefits record, by following this link:

G-Cloud 13 Customer Benefit Record

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 36 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, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

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 set the Term at more than 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:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)

- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

2.2.3 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 7 (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:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 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 as per clause 18.5 hereunder 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 14digit 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:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their 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 invoices under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the 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:

9.2.1 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

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 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

9.2.4 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:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 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:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 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:

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

10. Confidentiality

10.1 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 incorporated Framework Agreement clause
34. 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 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer 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:

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 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:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 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

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, 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:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 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

12.1.3 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:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 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

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

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

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

13.4 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 policies and all Buyer requirements in the Order Form.

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.npsa.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.npsa.gov.uk/protection-sensitive-information-and-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 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: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 Buyer requirements in respect of AI ethical standards.

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

13.8 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.

13.9 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.

13.10 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 at: https://www.gov.uk/government/publications/technologycode-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:

16.4.1 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

16.4.2 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 the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's 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:
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:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 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:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover 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:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

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

18.5.1 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

18.5.2 an Insolvency Event of the other Party happens

18.5.3 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:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 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); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
  24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 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:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 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

19.5.4 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

19.5.5 work with the Buyer on any ongoing work

19.5.6 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: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any 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 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 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 take the Term beyond 36 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:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 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:

21.8.1 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

21.8.2 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

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 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:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 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 30 consecutive days, 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 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer’s liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier’s liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

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:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 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:

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29. 2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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.

29.3 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.

29.4 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.

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

29.5.1 its failure to comply with the provisions of this clause

29.5.2 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

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

29.7 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:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 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, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services
Statement of Work for Provision of External Assistance to:
Classify and Catalogue Master Data used across the Defence Support domain.
Develop a Canonical Model of Support data.

Date: 01 November 23

TASK REQUIREMENT SUMMARY

Firstly to create a consolidated view of the master data used within Defence Support, including the systems in which they are mastered, and data management processes applied to them. Key metadata attributes of the master data entities are to be captured and recorded. Where master data conflicts are discovered between operational datasets/systems, proposals are to be made for their enduring resolution.

Secondly to develop a canonical model of Defence Support data, providing a common reference point for the delivery of future system integration messaging standards, and the presentation of underlying operational data within the Support Data Warehouse for data consumer exploitation in data marts (also known as the semantic layer).

BACKGROUND

As part of the initial stages of the **REDACTED TEXT under FOIA Section 43, Commercial Interests** programme several activities are required to be undertaken by the CIO to deliver a strong foundation from which to deliver high quality data. The initial primary deliverable is a new Support Data Warehouse (New SDW) with specific data pipelines and data marts to deliver business intelligence, periodic reporting and data for third parties. For the critical Support data held in the New SDW to be understandable to its customers (FLCs, Delivery Teams, analysts, industry, and others) it needs to be presented in a consistent manner, based on clear business terminology.
New Enterprise-Wide Support Systems (EWSSs) are being introduced to replace existing in-service applications across a wide range of sub-domains within Support e.g. inventory, movements. For the EWSSs in combination to deliver the required end-to-end processes, ownership of master data must be clear and commonly understood. Use of a Canonical Model in data integration has many advantages including reduced data translations, improved data consistency, integration flexibility and operational agility. The canonical model must assist in the application of specific industry data standards that are mandated by policy (for example the S-Series IPS specifications) or may have been adopted for convenience.

TASK REQUIREMENT DETAIL

Stream #1 – Master Data Catalogue

- Organise and run stakeholder workshops, analyse source documentation, and access system data libraries and directories to define, describe and catalogue master data across all support-related source systems, and define where such data is created and maintained within Defence Support.

Stream #2 – Master Data Recommendations

- Provide recommendations for the content, format, and processing to deliver an optimal master data management environment across Defence Support.

Stream #3 – Canonical Data Model

- Create, review and publish a canonical data model to be used in process modelling, data consolidation for creating data warehouses, the definition of data exchanges both internally between enterprise services and externally with industry.

These outputs will be supported by a combination of documents, visualisations, and demonstrations, as appropriate to show what has been done and how. Where data modelling is required, the outputs will need

to be captured in the CIO BizzDesign repository. It is expected that all outputs will be appropriately version controlled.

All work should actively evaluate and ingest work that has been undertaken previously, by product vendors, analytics teams, data quality activities or other initiatives, where provided by Defence Support CIO.

The work is expected to proceed data set by data set, beginning with those deemed most important and most easily accessible. There are an estimated 90,000 discreet data attributes across the Support enterprise systems that may potentially need to be catalogued. Of this only a small percentage represents Master Data in the Support domain. The work therefore will be approached in priority order as specified by the Support CIO.

The primary Support data sub-domains are Inventory, Engineering Maintenance, Warehousing and Movements. They represent the storage, handling and fitting of materiel which falls into a wide variety of categories, including large capital spares, munitions, medical products, consumables, and uniforms.
The Defence Chief Data Officer has procured, as part of a pan-defence Enterprise Agreement, the Informatica Data Catalogue tool, and there is already work underway to procure a pan-defence Reference Data Management product, which **REDACTED TEXT under FOIA Section 43, Commercial Interests** is intending to utilise to meet its own requirements in this area. Outputs generated the execution of this SoW may be ingested into those tools and into the wider Defence Support Business Architecture.

RATIONALE

The Defence Support IS landscape is fragmented between single service systems that exist to do the same thing, while gaps also exist between capabilities that have to be filled manually. The **REDACTED TEXT under FOIA Section 43, Commercial Interests** programme will mobilise the best of our existing systems in conjunction with new COTS products and redesigned processes to substantially improve on current Support IS and operational capabilities. This shared appreciation of the current and likely future state of technology will guide our data strategy, investment and plans across Defence Support.
A coherent design for and provision of Support Data is needed to provide clean data-centric services for consumption by users and applications. This has several parts: a strong foundation of accurate metadata; a well-developed representation of critical Support data and their lifecycle; repeatable data quality processes; clear data ownership exercised through strong data management processes. These will proceed from the rapid ingestion of near real-time and historic data sources, through consistent integration onto specialised data platforms and deliver immediate event creation, fast analysis, and transparent access to the resulting curated information.
This Statement of Work is to address the second element, the representation of critical Support data and their lifecycle, which will in turn support the remainder of the activities.
This programme of work will need to be delivered in time to support the introduction of the new EWSSs.
The outputs will involve co-ordination with the Major Projects team in Defence Support and teams within DE&S but will be delivered from and under the oversight of the Defence Support CIO.

SUPPORTING ACTIVITIES

In addition to the deliverables outlined in section 3 above, the following general activities are required in support of them:

- Contribute to team meetings, workshops, and peer-to-peer meetings to drive forward the specific output and the general agenda of the DefSp CIO.
- Engage with key consumers and stakeholders of Defence Support data to ensure that our intentions regarding cataloguing will fulfil reasonable external needs.
- Participate with the Defence CDO team who are co-ordinating the Data Catalogue deployment with Informatica and the definition of Defence data sub-domains, and data glossary entries. Engage with DE&S Digital to ensure alignment with similar activities for their other data domains.
- Prepare deliverables, where relevant, for both documentation and presentation material. Contribute to and deliver, where needed, those communications.
- Raise issues and identify opportunities for the exploitation of the Informatica platform in support of any activities.

GOVERNANCE

Project governance processes will be established throughout the three phases including:
There would be a kick off/ onboarding meeting to go through the implementation plan and deliverables in the first week of onboarding.

- Weekly progress reports from the project team/engagement lead
- Monthly updates for senior stakeholders
- Milestone reports and updated for all stakeholders and project sponsor.

Further governance details will be provided pending client feedback on the preferred approach and timing.

The Contract and all associated activity are subject to and governed by the internal governance structure of the Authority. The Supplier must always demonstrate adherence to this.

The Supplier will adhere to, as a baseline but not limited to, the governance and conditions outlined within the following DEFCONs; which are also included in the accompanying order form for this contract:

- DEFCON 658 – Cyber
- The Cyber Risk Profile for this requirement is Not Applicable (as set out by the Defence Cyber Protection Partnership (DCPP).
- As the Cyber Risk Profile for this Risk Assessment is Not Applicable, the supplier will need to complete a Risk Assessment for all subcontracted elements of this work. Awaiting cyber risk profile
- The Supplier must also complete a Supplier Assurance Questionnaire (SAQ) in relation to the risk assessment (reference RAR- 792277893).
- DEFCON 659A – Security Measures
- DEFCON 660 – Official Sensitive Security Requirements

ASSUMPTIONS

- Access to ModNet and the Informatica Catalogue on MODCloud will be provided as required.
- Access to the Defence Support BizzDesign repository will be provided as required.
- DefSp, DE&S Digital and Defence Digital staff will be accessible.
- Classification for all the data in the scope of work will be no higher than Official Sensitive.
- Scope will cover specific data sets to be provided by Def Sp CIO which will all be sourced from the Support Data Warehouse.
- Access to stakeholders will be provided within reasonable timeframes to enable planned dates to be met. This includes organisation and attendance at workshops as required by the **REDACTED TEXT under FOIA Section 43, Commercial Interests**.
- Acceptance authority for deliverables will be the CIO Data Lead supported by the wider Data Team. The CIO Data Lead will support review and acceptance of deliverables within Seven working days after which, the deliverable will be assumed as approved.
- Approximately 10%, or less, of 90,000 discrete data attributes represent the Master Data in the Support domain to be analysed and catalogued. The domains to be included within the analysis and modelling are Inventory, Assets, Engineering Maintenance, Warehousing and Movements.
- At the end of the first three weeks of the project (Mobilisation) both Defence Support and Eviden will confirm and agree
    - the detailed scope of the domains and systems to be analysed and documented for both Draft and Final versions of each deliverable (payment milestone); and
    - the delivery, content and format of the deliverables;

  limited to the indicative resource levels.

- Third parties tasked with maintaining current systems will provide information about data and metadata as required. The CIO will use reasonable endeavours to get the information being requested. In the event that the data is not available in time to meet the relevant milestone Eviden reserve the right to remove that element from the milestone.

- The following are out of scope:
    - The implementation and ongoing management of MDM Governance across Defence Support.
    - The development of canonical model components relating to transactional and non-MDM related integration requirements i.e. a transactional data record that is relevant for point-to-point integration between two current information systems but does not represent a significant data entity within the canonical or master data models. For example, an asset may have an asset history entity associated with it in the canonical model, but the exhaustive list of historical events that may be associated with an asset will not be modelled, just the representation of how a historical event is described in data terms.
    - Provision of any support required to maintain, extend or modify the master data catalogue or canonical data model beyond the duration of this contract.

An expanded list of assumptions and dependencies is provided in the Annex A.

SKILLS AND RESOURCING

It is anticipated that to produce the deliverables, personnel with suitable skills in data analysis and modelling will be provided, with experience in wider data management.

TIMESCALES AND REPORTING

Detailed tasks and timescales are to be agreed with the customer including a high-level timeline of deliverables.
The anticipated period of tasking is 19 Feb 24 to 30 Jun 24, phased as described above and subject to review hereafter.
The delivery agent is to provide fortnightly updates on progress with burn rate on outputs and consumption of budget to the relevant CIO representative. Risk and issue logs are to be maintained and reported in order to deliver services to meet contractual requirements. Day to day management and supervision of resource will be carried out by the delivery agent.

PAYMENT MECHANISM

The Authority is introducing a milestone payment plan where 100% of each milestone will be paid upon completion.
Should a milestone be outstanding against its delivery date, a 20% retention in the milestone value, will apply, until such time that the milestone has been completed, submitted and accepted by the Authority.

KEY PERFORMANCE INDICATOR /PERFORMANCE INCENTIVE

Milestone Payments may be subject to an overall 20.00% retention against each milestone value if milestone delivery isn't complete as per table 1 in Schedule 2. This will mean that the supplier may receive 100% on completion of each milestone or may receive 80% milestone payment only if completion date not met. The remaining 20% would be paid on milestone completion.

SECURITY & CYBER RISK REQUIREMENTS

The Cyber Risk Profile for this Project has been assessed by the DCCP Team and has deduced a profile of Not Applicable for this procurement. The Supplier will need to complete an SAQ. If Compliance is not

met, the contract cannot be awarded until a Contract Implementation Plan has been approved by the Authority.

GFX

The Supplier will be issued with laptop devices, that remain the property of the Authority, and are supplied for the sole use of accessing MOD applications and services for use on this project. Use of the devices and access to data mandates the supplier must adhere to MOD security policy.

It is anticipated that the laptop devices will be issued to the identified team members within ten business days of the Supplier's submission of the signed Tasking Order Form. In order to expedite the contract start date the Supplier must submit the following information regarding their team members to the Authority's designated Commercial Officer along with the signed order form:

Full Name

Date of Birth

Address (that the laptops will be delivered to)

Contact telephone number

To facilitate a seamless transition, the Supplier must provide contact details (as listed above) of any changes to personnel (approved by the Authority) no later than ten business days prior to their commencement of any work performed under the Contract. It is the Supplier's responsibility (at their own cost) to securely deliver the laptop device to the new team member.

At the close of the contract, a review will take place to ensure laptop devices and any accompanying paraphernalia are returned in the same condition that they were issued, subject to fair wear and tear. All documents, artefacts, information pertaining to the delivery of this programme needs to be returned to the Authority or destroyed at the MOD's request.

SOCIAL VALUES

Where opportunities arise during the contracted activities, the supplier will be expected to demonstrate their commitment to:

a. Fighting climate change and working toward zero emissions.

b. Promoting equal opportunity.

COMMERCIAL OFFER

Commercial offer is made on a firm price basis, using previously agreed GCloud 13 rates and terms. Delivery fees for the delivery of the project described in this proposal are shown below. Travel and expenses are included on an assumed basis of working in Bristol for a maximum of two days per week.

Fees and Charges ex VAT	Amount (GBP)
Delivery Fees inclusive of standard expenses to Bristol	£ 820,072.00
Exceptional travel allowance to other MOD sites as suggested by the Authority (6 days for 2 people)	£ 1,560.00
Total Price	**£ 821,632.00**

Payment milestones related to delivery fees are detailed below and in Schedule 2. Where exceptional travel has been requested and approved by the Authority, any incurred expense will be added to next applicable invoice.
Invoices for fees will be raised in accordance with the following payment milestones and payable in accordance with the terms defined under the GCloud 13 Agreement.

Indicative effort is provided for information purposes only and will not be used for any other purpose . All milestone payments will be invoiced on the full milestone value as stated.

REDACTED TEXT under FOIA Section 43, Commercial Interests

OUTCOMES, REQUIREMENTS & DELIVERABLES

The Table below outlines the key activities and deliverables involved in completing the Authority's outcomes, the deliverable date and trigger for invoicing against the milestones.

Ref	Authority's desired outcome	Service requirement	Deliverable Date(s)	Charges (exc VAT)	Invoice / Trigger Cycle
MS0	**Mobilisation**	• Workshops / sessions held to ○ Identify key stakeholders and share workshop plans/proposals. ○ Agree scope and approach to delivery / assign milestones. ○ Re-baseline the delivery plan ○ Agree format and content of deliverables. • Delivery team gets access to the required documentation, and MOD systems	8 Mar 2024	Non-billing milestone	Acceptance of written mobilisation report.
Master Data Catalogue					
MS1	**Draft Master Data Catalogue**	• Capture and document MDM data by source system within specified Support data domains identified during mobilisation. • Populate draft catalogue and hold regular feedback sessions with stakeholders. Key outputs per domain will include: ○ Domain definition and business scope/processes supported. Interrelationship between domains. ○ Definition of master data logical entities and key attributes including name, description, format, source system (where mastered/captured and where updated), draft CRUD matrix defining relationship between high level processes and master data.	31 Mar 2024	£202,120.00	Acceptance of Draft Data Catalogue, including: • Initial domain data entities in line with Assumptions • Data lineage and data sources for selected domain • Entity format e.g., synonyms, constraints, default and example values. Format to be confirmed in Mobilisation e.g. BizzDesign, MS Word/MS Excel

Ref	Authority's desired outcome	Service requirement	Deliverable Date(s)	Charges (exc VAT)	Invoice / Trigger Cycle
		○ Description of source systems for Master Data entities and attributes including business processes supported, master data and high-level data flows between systems. • The delivery format of the above deliverables to be agreed during mobilisation. • Complete and share draft MDM data catalogue.			
MS2	**Final Master Data Catalogue**	• Capture and document final MDM data entities and attributes. • Complete and share final MDM data catalogue. • Revise and issue approved data catalogue. • Circulate to key stakeholders. • Complete stage closure and sign off.	30 Apr 2024	**REDACTED TEXT under FOIA Section 43, Commercial Interests**	Acceptance of Final Master Data Catalogue, including: • Definition and content of entities and attributes, • Data lineage and data sources • Entity format e.g. synonyms, constraints, default and example values. Format to be confirmed in Mobilisation e.g. BizzDesign, MS Word/MS Excel
Master Data Model Recommendations					
MS3	**Draft Master Data Model Recommendations**	• Initiation, mobilisation of stakeholders and agree milestones. ○ Initiate workshops with stakeholders. ○ Review the results of Draft Master Data Catalogue to identify and prioritise work focusing on key problem areas within the MDM landscape within DE&S. • Develop Draft Recommendations for Master Data Model. ○ Analyse issues and create draft recommendations for key/high priority areas.	30 Apr 2024	**REDACTED TEXT under FOIA Section 43, Commercial Interests**	Acceptance of Draft Master Data Model Recommendations as to how current master data management could be modified to make Support data more consistent, comprehensible, and useable and to resolve duplicate or incomplete master data record sets. Format to be confirmed in Mobilisation e.g. MS Word/MS PowerPoint

Ref	Authority's desired outcome	Service requirement	Deliverable Date(s)	Charges (exc VAT)	Invoice / Trigger Cycle
		○ Initiate workshops to walk through recommendations. ○ Review the and revise as draft recommendations.			
MS4	**Final Master Data Model Recommendations**	• Complete final recommendations ○ Create draft recommendations for lower priority areas. ○ Initiate workshops to walk through recommendations. ○ Review the draft recommendations. Typical recommendations for delivering Master Data Model include: ○ Where possible, resolution of multiple sources of master data creation – one source being primary, all others secondary, to ensure one version drives the generation of that data. ○ Development of a standard set of rules for all applications handling Master Data (creation or amendment) to ensure consistency across the application landscape. This includes both entity and attribute content and format. ○ Development of business process rules to ensure validation of Master Data is conformed with a core standard. Where possible automation of those rules during entity creation and/or amendment. ○ Develop final recommendations. • Review and finalise recommendations with stakeholders.	30 Jun 2024	**REDACTED TEXT under FOIA Section 43, Commercial Interests**	Acceptance of Final Master Data Model Recommendations as to how current master data management could be modified to make Support data more consistent, comprehensible, and useable and to resolve duplicate or incomplete master data record sets. To include recommendations as to how master data values could be managed in the future landscape being delivered by REDACTED TEXT under FOIA Section 43, Commercial Interests. Format to be confirmed in Mobilisation e.g. MS Word/MS PowerPoint

Ref	Authority's desired outcome	Service requirement	Deliverable Date(s)	Charges (exc VAT)	Invoice / Trigger Cycle
		○ Issue recommendations and project definitions to stakeholders (IT and business) ○ Initiate workshops to walk through final recommendations. ○ Review the and revise final recommendations. ○ Publish recommendations for future action. ○ Complete stage closure and sign off.			
Canonical Data Model					
MS5	**Draft Canonical Data Model**	• Initiation, mobilisation of stakeholders and agree milestones. • Organise and run workshops to complete conceptual integration model, confirm priority, scope, format, and tools for Canonical Data Model with Support CIO, initiate canonical model build. ○ Develop conceptual integration model and issue for review. ○ Confirm canonical data model scope, format, and tools. Make tools available to project team. ○ Confirm scope and priority of analysis/model development with Support CIO ○ Agree use of architecture tools and appropriate architecture model components and conventions. • Initiate build of Draft Canonical Data Model ○ Develop and document draft Canonical data model. ○ Initiate build of canonical model. Key deliverables to be confirmed during mobilisation. Typically, these include: ○ Definition of current systems and integration requirements (input to final model)	31 May 2024	**REDACTED TEXT under FOIA Section 43, Commercial Interests**	Acceptance of the Draft Canonical Data Model to include: • Conceptual Integration Model - Conceptual / Logical model used to identify and define all the domains to be included in the canonical model. • Draft Canonical model for selected data domains (to be agreed in Mobilisation) • The definition of rules that will allow current data attributes to be transformed into their canonical representation. Format to be confirmed in mobilisation e.g. BizzDesign repository following ArchiMate notation

Ref	Authority's desired outcome	Service requirement	Deliverable Date(s)	Charges (exc VAT)	Invoice / Trigger Cycle
		○ Dataflow/Integration diagrams for current systems (input to final model) ○ Conceptual Integration Model - Logical model diagram used to define and validate scope potentially segregated by business data domain. ○ Canonical Model Diagram – detailed model diagram identifying logical integration flows. ○ Logical integration data flow definitions including (if available) source and end target systems, frequency and latency (real time, near real time, batch), data content/key attributes, data format, business and transformational rules, volumes, growth forecast. ○ Define transformation rule models for core data attributes.			
MS6	**Final Canonical Data Model**	• Complete and review draft Canonical Data Model ○ Complete draft Canonical Data Model. ○ Initiate workshops to walk through model components domain by domain. ○ Review the and revise draft model. • Publish and approve Canonical Data Model ○ Publish Canonical Data Model. ○ Initiate workshops to review model domain by domain. ○ Approve Canonical Data Model ○ Complete stage closure and sign off. ○ Complete programme closure review and sign off.	30 Jun 2024	**REDACTED TEXT under FOIA Section 43, Commercial Interests**	Acceptance of Final Canonical Data Model for domains agreed in Mobilisation. Format to be confirmed in mobilisation e.g. BizzDesign repository following ArchiMate notation

LOCATION

Bristol is the office base for the Defence Support CIO team, but the work can be delivered largely remotely with periodic face-to-face engagements.

Schedule 2: Call-Off Contract charges
For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform 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:

Table 1 Fees and Charges ex VAT

Fees and Charges ex VAT	Amount (GBP)
Delivery Fees inclusive of standard expenses to Bristol	£ 820,072.00
Exceptional travel allowance to other MOD sites as suggested by the Authority (6 days for 2 people)	£ 1,560.00
Total Price	**£ 821,632.00**

Table 2 Milestone Payment Subject to KPI Retention
REDACTED TEXT under FOIA Section 43, Commercial Interests

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 Clause 2 (Services) 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 Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
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 UK 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 Call-Off Contract 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 (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK 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.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
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 the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
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 RM1557.13 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 Clause 2 (Services) 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.

UK GDPR	The retained EU law version of 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.
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 ● a Dun & Bradstreet rating of 10 or less
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 Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.

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 Schedule 6.
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 UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK 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: pseudonymisation 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 Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
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-controlsche ck-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: UK GDPR Information
This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

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 TEXT under FOIA Section 40, Personal Information** their contact details are: **REDACTED TEXT under FOIA Section 40, Personal Information**

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

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Identity of Controller for each Category of Personal Data	**The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: ● Supplier personnel data for onboarding purposes

Duration of the Processing	Onboarding data which will be available upon contract start and potential available throughout
Nature and purposes of the Processing	Onboarding processing
Type of Personal Data	▪ Full Name • Date of Birth • Address (that the laptops will be delivered to) • Contact telephone number

Categories of Data Subject	Supplier Staff to be onboarded by the Buyer containing personal data
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	Onboarding – this data will be removed after project completion

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the **Supplier and Buyer**:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the **Supplier's and Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

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

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

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

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

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

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

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

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

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

(i) are aware of and comply with their ’s duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

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

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

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

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

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

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

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

(b) all reasonable assistance, including:

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

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

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

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

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

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

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

4. Audit

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures

relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

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

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the

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

(b) if in the view of the Information Commissioner, the Supplier is responsible for thePersonal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner,then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

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

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Termination

8.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (Joint Controller Agreement), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

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

Annex A:

Assumptions and Dependencies:
Assumptions:
The following assumptions have been made in relation to this proposal:

A1. Plans and milestones will be formally agreed between Defence Support and Eviden as part of project initiation within the first two weeks of the project.

A2. All MOD and Eviden resources required to initiate the project can be mobilised within the planned timelines.

A3. Requested Defence Support resources can be made available as required under the agreed plan.

A4. Access to Defence Support management to facilitate the initiation of work and provide stakeholder details is provided.

A5. Work can begin on local (Eviden) laptops and transferred to MOD laptops once made available, however MOD data handling needs to be only on MOD laptops.

A6. The detailed content and format of deliverables will be agreed between Defence Support and Eviden during the first four weeks of the project.

A7. Relevant information related to existing master data attributes and related source systems is available to the team from the start of the project.

A8. Systems of record include documented data models that describe the relevant Master Data.

A9. It is assumed that approximately 10%, or less, of 90,000 discrete data attributes represents the Master Data in the Support domain to be analysed and catalogued in Stage 1.

A10. It is assumed that the domains to be included within the analysis and modelling are Inventory, Assets, Engineering Maintenance, Warehousing and Movements

A11. The definition of transformation rules applying to data to align with the canonical model can be achieved by the implementation of rule standards aligned to data types and content and, where applicable, driven by existing internal and external standards.

A12. All work required can be undertaken by resources cleared to SC level only.

Dependencies:
The following dependencies have been identified in relation to our proposal and commercial offer:

D1. At the end of mobilisation phase both MOD and Eviden will confirm and agree the detailed scope of the domains and systems to be analysed and documented.

D2. Provision of MODNet access and associated MOD data modelling software will be made available to Eviden team members for the duration of the engagement at no cost to Eviden.

D3. MOD will provide appropriate source information to support analysis of Master Data for instance, documentation about source systems, internal data structures, existing interface specifications during the mobilisation phase of the project.

D4. MOD will provide details of stakeholders assigned to support the project within the mobilisation phase of the project and support the organisation of workshops with these stakeholders in accordance with the schedule identified by the Eviden team.

D5. At the conclusion of mobilisation all required stakeholders identified by MOD will confirm their attendance for workshop sessions to the provide schedule.

D6. MOD will provide be able to provide appropriate source information to support creation and approval of Canonical Model entities.

D7. Third parties tasked with maintaining current systems can provide information about data and metadata as required within 5 days of that information being requested.