

DEFFORM 8 (Edn 04/22)

OFFICIAL



Ministry
of Defence

Angus MacKay
Def Comrcl Head Office Business Partner 3-1

Ministry of Defence
Kentigern House
65 Brown Street
Glasgow G2 8EX
United Kingdom
Email: Email:
Angus.Mackay240@mod.gov.uk

Corporate Project Solutions Limited
Jubilee House
Third Avenue
Marlow
Bucks
SL7 1EY

Your Reference:

Our Reference:
707087450
Date: 22 March 2023

FAO: **redacted**

Dear Sir,

Offer Of Contract 707087450 for External Assistance to maintain Project Online (POL) Instance and automated reports using MS PowerBI within Defence People Team (DPT) through G-Cloud 13 Framework Agreement (RM1557.13).

- Reference A. Message "Ministry of Defence - G-Cloud13 - Clarification Questions for External Assistance to maintain Project Online and PowerBI" sent by the Authority on 6 March 2023 and updated on 9 March 2023.
- Reference B. Your message "RE: Ministry of Defence - G-Cloud13 - Clarification Questions for External Assistance to maintain Project Online and PowerBI - v3.1", sent by email on 14 March 2023.
- Reference C. Your document "20230309-SOR_POL_EA_Approved-V3.1 - CPS Response", attached to Reference B.
- Reference D. Your document "CPS Response", attached to Reference B.
- Reference E. Your message "RE: Ministry of Defence - G-Cloud13 - Clarification Questions for External Assistance to maintain Project Online and PowerBI - v3.12", received by email on 20 March 2023.

1. Further to reference A, B, C and D and as clarified in Reference E, I am to inform you that the Authority now makes the following Offer of Contract to You. We are accepting the Pricing Schedule as it has been updated in Reference E and that is reproduced here in the Schedule Two.

2. Please note the details on the attached Statement of Requirement and Pricing Schedule and note that the Prices quoted are exclusive of VAT.
3. Please sign and return the enclosed final version of the Contract within 10 working days of the date of this letter to acknowledge your acceptance of the Terms and Conditions.
4. Please note that no Contract will come into force until both parties have signed it. The Authority will countersign the Contract and return a copy of the same to you.
5. Payment will be made in accordance with the attached Terms and Conditions. If your company has not already provided its banking details to the Defence Business Services (DBS) Finance Branch, please complete the Form CX723, which is available from the Gov.uk (<https://www.gov.uk/government/publications/dbs-finance-payments-nominate-a-bank-form>) and forward to DBS Finance, Walker House, Exchange Flags, Liverpool, L2 3YL.
6. The Authority may publish notification of the Contract and shall publish Contract documents under the FOI Act except where publishing such information would hinder law enforcement; would otherwise be contrary to the public interest; would prejudice the legitimate commercial interest of any person, or might prejudice fair competition in the supply chain.
7. If you wish to make a similar announcement you must seek approval from the named Commercial Officer.
8. Under no circumstances should you confirm to any third party that you are entering into a legally binding contract for the provision of Licenses for Egress Workspace to assist with Home Office Disregard scheme prior to both parties signing the Terms and Conditions, or ahead of the Authority's announcement of the Contract award.

Yours sincerely,

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

DEFFORM 8 (Edn 04/22)	1
G-Cloud 13 Call-Off Contract.....	3
Part A: Order Form	4
Part B: Terms and conditions	12
Schedule 1: Services - Statement of Requirement.....	31
Schedule 2: Call-Off Contract charges – Pricing Schedule	43
Schedule 3: Collaboration agreement – Not applicable	45
Schedule 4: Alternative clauses	45
Schedule 5: Guarantee – Not applicable.....	49
Schedule 6: Glossary and interpretations.....	49
Schedule 7: UK GDPR Information	69
Annex A. The project specific DEFCONs that apply to this Contract.....	69
Annex B - Security Aspects Letter	71
Annex to Security Aspects Letter	73
Annex C. DEFFORM 111	82

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	390451983098439
Call-Off Contract reference	707087450
Call-Off Contract title	External Assistance to maintain Project Online
Call-Off Contract description	External Assistance to maintain Project Online (POL) Instance and automated reports using MS PowerBI within Defence People Team (DPT).
Start date	01/04/2023
Expiry date	31/03/2024
Call-Off Contract value	£70,000.00 ex VAT
Charging method	As per DEFCON 522 (Edn. 11/21) - Payment and Recovery of Sums Due
Purchase order number	707087450

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 contract with square brackets.

From the Buyer	Ministry of Defence – Head Office Commercial Angus MacKay Def Comrcl Head Office Business Partner 3-1 Ministry of Defence Kentigern House 65 Brown Street Glasgow G2 8EX United Kingdom Email: Angus.Mackay240@mod.gov.uk
To the Supplier	Corporate Project Solutions Limited Jubilee House Third Avenue Marlow Bucks SL7 1EY FAO: redacted redacted redacted Company number:
Together the ‘Parties’	

Principal contact details

For the Buyer:

Title: Commercial Officer

Name: Flavia Fanchin Moedinger

Email: flaviafanchin.moedinger100@mod.gov.uk

Phone: 03001 58 5676 (Skype)

For the Supplier:

Title: redacted

Name: redacted

Email: redacted

Phone: redacted

Call-Off Contract term

Start date	This Call-Off Contract Starts on 1st April 2023 and is valid for 12 months .
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>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).</p>
Extension period	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 1 months written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>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.</p>

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	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> • Lot 3: Cloud support
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <ul style="list-style-type: none"> • As listed in the Schedule One – Statement of Requirement and Schedule Two – Pricing Schedule
Additional Services	As listed in the Schedule One – Statement of Requirement and Schedule Two – Pricing Schedule

Location	The Services will be delivered as per Schedule One – Statement of Requirements.
Quality Standards	The quality standards required for this Call-Off Contract are as per Schedule One – Statement of Requirements.
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are as per Schedule One – Statement of Requirements.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as per Schedule One – Statement of Requirements.
Onboarding	The onboarding plan for this Call-Off Contract is as set out on the Supplier's G-Cloud 13 Marketplace Service Definition.

Offboarding	The offboarding plan for this Call-Off Contract should be presented by the provider three months before the expiry date.
Collaboration agreement	Not applicable.

<p>Limit on Parties' liability</p>	<p>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 £ 70000,00 per year.</p> <p>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 150% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of 150% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p>
<p>Insurance</p>	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> • [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 for each individual claim or any higher limit the Buyer requires (and as required by Law)] • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
<p>Buyer's responsibilities</p>	<p>Not applicable.</p>
<p>Buyer's equipment</p>	<p>The Buyer's equipment to be used with this Call-Off Contract includes one MOD laptop</p> <p>Reason: to access Project Online for support and maintenance.</p>

Supplier's information

Subcontractors or partners	The provider should inform the Authority of the Supplier's Subcontractors or Partners working to deliver this requirement.
-----------------------------------	--

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 as per DEFCON 522 (Edn. 11/21) - Payment and Recovery of Sums Due
Payment profile	The payment method for this Call-Off Contract is as per DEFCON 522 (Edn. 11/21) - Payment and Recovery of Sums Due
Invoice details	The payment method for this Call-Off Contract is as per DEFCON 522 (Edn. 11/21) - Payment and Recovery of Sums Due
Who and where to send invoices to	The payment method for this Call-Off Contract is as per DEFCON 522 (Edn. 11/21) - Payment and Recovery of Sums Due
Invoice information required	The payment method for this Call-Off Contract is as per DEFCON 522 (Edn. 11/21) - Payment and Recovery of Sums Due
Invoice frequency	Invoice will be sent monthly to the Contract Manager.
Call-Off Contract value	The total value of this Call-Off Contract is £70,000.00
Call-Off Contract charges	The breakdown of the Charges is listed in the Schedule Two – Pricing Schedule.

Additional Buyer terms

Performance of the Service	Not applicable.
Guarantee	Not applicable.
Warranties, representations	Not applicable.
Supplemental requirements in addition to the Call-Off terms	Not applicable.
Alternative clauses	The Alternative Clauses in the Schedule 4 are not applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms	Within the scope of the Call-Off Contract, the Authority will include the DEFCONs listed in the Annex A.
Personal Data and Data Subjects	As per DEFCON 532A (Edn 05/22) - Protection of Personal Data where Personal Data is not being processed on behalf of the Authority
Intellectual Property	As set out on the Supplier's G-Cloud 13 Marketplace Service Definition.
Social Value	Not applicable.

1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a CallOff 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	[Enter name]	Angus MacKay
Title	[Enter title]	Senior Commercial Officer BP3
Signature		
Date	[Enter date]	[Enter date]

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

Part B: Terms and conditions

1. Call-Off Contract Start date and length

- Order Form.
- 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 invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed 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-securityclassifications>
 - 13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:
<https://www.cpni.gov.uk/content/adopt-risk-managementapproach> and Protection of Sensitive Information and Assets: <https://www.cpni.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.

- Form.
- 13.7 The Buyer will specify any security requirements for this project in the Order
 - 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/technology-code-of-practice/technology-code-of-practice>
 - 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
 - 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
 - 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN
- if the PSN
- Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
 - 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 CallOff 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 Requirement

MS Project Online (POL) and PowerBI Project Management and Reporting Tool External Assistance Support

STATEMENT OF REQUIREMENT (SOR)

Version 3.1

Statement of Requirement for POL and PowerBI P3M Tools

Date 28/02/23

VERSION CONTROL

Date Issued	Version	Author	Reason for Change
16/05/22	1.0	Sam Kinsey-Briggs	Initial Draft
04/07/22	2.0	Sam Kinsey-Briggs	Initial Draft V2
23/08/22	2.5	Sam Kinsey-Briggs	Draft for DPT circulation
30/09/22	3.0	Zoe Restall	Final version for Commercial action
3/02/23	3.0		Update for 2023
07/03/23	3.0	Zoe Restall	Updated for Commerical action
08/03/23	3.1	Zoe Restall	Amendment to part 2 and annex C

Contents

Part 1 – GENERAL DESCRIPTION

- Background
- Business Context
- Operating Process
- Assumptions
- Aims
- Task Description
- Timeline

PART 2 – DETAILED TASK DESCRIPTION

PART 3 – DOCUMENT SUPPORT

GLOSSARY

CONTRACT MANAGEMENT

Original Task No

PROJECT ONLINE INSTANCE DEVELOPMENT COSTS

Part 1 – General Description

Background

To meet Defence and Chief of Defence People's (CDP) needs for effective Portfolio Management and Project Delivery across the Defence People Team (DPT) and the People Function, the People Portfolio Office (PPfO) have a role to improve Project Delivery processes and expertise across the DPT. By doing so, CDP will have better means to plan and manage resources efficiently, hold to account and supply assurance that outputs are being achieved.

This SOR outlines the assistance required to maintain, improve and enhance the Microsoft (MS) POL Instance¹ and associated PowerBI reporting² already within the DPT, with the aim of increasing the effectiveness of Portfolio and Project Management, reporting, transparency and holding to account. The PPfO has recently introduced POL to the DPT and associated PowerBI reports that are being used to support key management and programme/project boards³. As with any technology it is critical to stay aligned not only within Defence, guided by Defence Digital, but also to take advantage of new and emerging technologies such as Project for the Web (PftW) and Dataverse. Having used the initial POL Instance over the last few months, the DPT **now needs a period of consolidation where technical support is required** to provide routine maintenance and continue staff training to develop the Portfolio Office and wider DPT SQEP.

The PPfO requires continued User and Administrator training (for both POL and PowerBI) to develop sufficient Suitably Qualified and Experienced People (SQEP).

¹ Currently 2 POL instances, 1 live and 1 test with no add ons/plugin ins, only non-standard configuration is minimal through Java Script.

² 5 main reports currently being used, this is expected to increase.

³ Dashboards have been used for DPLT, Management Boards and PLT since Aug/Sep 22.

The business needs are as follows:

- To consolidate and improve business processes.
- To ensure routine maintenance and administration of the POL Instance is conducted and to provide knowledge transfer so that the product can be developed and refined in the future.
- Have the access and ability to analyse data (including the use of AI and data analytics) across the whole organisation (DPT) but that can better link in to the Front Line Commands and other TLBs. This visibility of statistical and trend analysis will support the DPT to enable it to fulfil its commitments to wider Defence, including to relevant Defence Tasks and Defence Enabling Outputs.
- To be able to integrate with other Digital Tools such as DAT, CP&F, PB&F⁴, CSA⁵, GOST, PARMIS, Risk Flightpath Tool ⁶etc – in the future, it is critical to collect data and consolidate processes so that this can be looked at in detail in the future once more SQEP has been developed amongst the team.
- To ensure that the DPT has a sustainable and resilient pathway to adopt future technology changes as they are rolled out (such as Dataverse and Project for the Web (PftW)), to continue the development of portfolio management services.
- To ensure Change Requests and all Bugs and Ideas from the PPfO Backlog are considered and actioned against priorities as set by the PPfO. This will be monitored via monthly updates and automated reports using POL and PowerBI reports.
- To ensure data quality and accuracy, monthly data analytics and site usage analysis will be reported to identify data shortages and also low-quality data to assist the business in collecting better quality data to enable analysis.

Business Context

As the business and PPfO matures and uses POL and the associated PowerBI reports, it will be necessary to ensure that the POL instance is maintained, revised and improved as the business and various processes evolve across the DPT. This will require contractor support to maintain MS POL Instance as well as to make the necessary updates to the associated PowerBI templates and reports. There is a requirement for ongoing technical support and maintenance as well as ongoing training as the DPT develops the necessary skills across the Directorates and P3M cadre. The DPT currently has 400+ POL users registered with 120+ lines of activity on POL.

Operating Process

The initial benefits of transparency and time saved on resources is yet to be realised as there are still Programmes and Projects across the DPT who are embedding the tool in their day-to-day business. This benefit will only be realised in due course and over time once all teams are using the tool and importantly, providing detailed and accurate data. This also benefits from breaking down projects into time and resource-based tasks, to provide visibility of who and what is being delivered in an agreed timeframe (BAU projects will also benefit from this sort of disciplined behaviour).

⁴ [Finance Reporting - PB&F \(sharepoint.com\)](#)

⁵ [Control Self-Assessment Tool](#)

⁶ [JSP 892 \(sharepoint.com\)](#) – Risk Flightpath Tool sits within JSP 892

Tracking of Business Plan outputs ([DPT BP23 Commission](#)) as well as wider People Leadership Team (PLT) level discussions will be enhanced in due course once the wider DPT uses the tool and provides the data. Retention and staff engagement should improve over time as the tool becomes part of routine business and staff are able to fully realise the benefits of automated reporting, as with any new technology, it will take time to effect and embed a culture change. Having used the system for over 6 months and having drawn on lessons from the Army and Navy rollout, now is the time to focus on maintaining POL and supporting users to develop relevant skills and knowledge which will support further positive changes and developments within the DPT. This will also support restructuring and outputs from the DPT P3M centralisation work and remodelling.

Assumptions

The DPT and PPfO are in the process of continued improvements, relating to business process and business outputs and any upgrades to systems must be aligned with these continued improvements. **Collection of good quality data in POL is critical** to enable the production of automated reports, it is therefore assumed that all Directorates within the DPT will continue to use this single tool for data input/collection and collation and improve the quality and quantity of data. Training for personnel in using the data collection tool is ongoing and any changes will also need to be communicated to ensure all users are fully conversant with any amendments or upgrades. **Communication of change to systems and associated processes will be critical** and the Communications team ([POL Comms](#)) will be essential in supporting this outcome supported by Business Managers, Chiefs of Staff and outer offices, as well via P3M personnel⁷ cross the DPT. It is assumed that because of Defence's wider Microsoft suite of tools and ongoing contract, that PftW and Dataverse will be the logical transition, from POL to PftW as it will not just be data, but structure, process and accessibility to O365 tools, power platforms etc. This natural next step as the migration of data from POL to PftW should be simple and easy with the systems being able to synchronise information and work alongside each other providing more flexibility and a better user experience. It is recognised, that this migration may still be years away, but early acknowledgement is critical to ensure the PPfO stays abreast of wider Defence and Industry standards.

Aims

To maintain the DPT POL Instance and PowerBI report suite to improve automated reporting and a coherent view across the DPT Portfolio.

To support the use of POL through maintenance, bug fixes and provision of training to develop knowledge amongst a wider range of POL users.

Task Description

⁷ P3M Business Partners (in the future DPT centralised model) will be well placed to add much value in each Directorate as they upskill and develop their POL and PowerBI SQEP.

Tasks will include maintaining and enhancing the DPT POL Instance by fixing bugs, tackling key backlog items and Change Requests from the POL Roadmap as well as providing user support and training. This routine maintenance activity, and all associated reporting will be managed using the DPT POL Instance so that all associated reporting can be used to provide live updates for Senior Leadership throughout this period. Throughout this period of consolidation and routine maintenance there will be a need to ensure compliance and adherence to industry standard and alignment with [Continuous Improvement Assessment framework](#). A full description of the task is contained in Part 2 of this document. All access to DPT POL will be done through an issued MOD device and all users must hold a minimum of SC Clearance.

Timeline

Routine. There will be a 1-year maintenance contract which will involve maintaining POL and associated PowerBI reports, fixing bugs, supporting users and providing training for POL and Power BI.

Reporting Arrangements

The following personnel are stakeholders in this project and their specific roles for the project are annotated:

Post/Role	Name	Email	Project Role
DPT COS	Lee Cagna	Lee.cagna627@mod.gov.uk	SRO
Hd PPfO	Mike Boyle	Mike.boyle524@mod.gov.uk	Project Sponsor
PPfO Ops & Plans	TBC	TBC	Overall Development
Project support lead	Zoe Restall	Zoe.Restall823@mod.gov.uk	Overall development
Mil HRS PO	Tom Varco	Thomas.varco100@mod.gov.uk	Senior User and technical advisor
Project Lead	Emily Kent	Emily.Kent105@mod.gov.uk	Comms and Project delivery/management

PART 2 – DETAILED TASK DESCRIPTION

The task and contract will be set for 12 months in which time the following key deliverables will be achieved, there may be a necessity to shift key deliverables into different months, depending on external factors or dependencies. The PPfO backlog will be used to manage any outstanding backlog issues and these key deliverables as well as any emerging backlog issues raised via Bugs & Ideas and Change Requests.

	April 23	May 23	June 23	July 23	Aug 23	Sept 23
Site maintenance, user assistance & bug fixes	2 days User assistance – 1 day Site maintenance and bug fixes – 1 day	<u>4 days</u> User assistance – 2 days Site maintenance and bug fixes – 2 days	<u>4 days</u> User assistance – 2 days Site maintenance and bug fixes – 2 days	5 days User assistance – 2 days Site maintenance and bug fixes – 3 days	2 days User assistance – 1 day Site maintenance and bug fixes – 1 day	<u>4 days</u> User assistance – 2 days Site maintenance and bug fixes – 2 days
User training POL & Power BI		1 day POL training – 0.5 day Power BI – 0.5 day	1 day POL training – 0.5 day Power BI – 0.5 day	1 day POL training – 0.5 day Power BI – 0.5 day	.	
Other						

	Oct 23	Nov 23	Dec 23	Jan 24	Feb 24	March 24
Site maintenance, user assistance & bug fixes	<u>4 days</u> User assistance – 2 days Site maintenance and bug fixes – 2 days	<u>4 days</u> User assistance – 2 days Site maintenance and bug fixes – 2 days	2 days User assistance – 1 day Site maintenance and bug fixes – 1 day	3 days User assistance – 1.5 days Site maintenance and bug fixes – 1.5 days	<u>4 days</u> User assistance – 2 days Site maintenance and bug fixes – 2 days	2 days User assistance – 1 day Site maintenance and bug fixes – 1 day

User training POL & Power BI	1 day	1 day		1 day	1 day	
	POL training – 0.5 day	POL training – 0.5 day		POL training – 0.5 day	POL training – 0.5 day	
	Power BI – 0.5 day	Power BI – 0.5 day		Power BI – 0.5 day	Power BI – 0.5 day	
Other						

This work will be managed using the DPT POL Instance and all associated reporting will be used to provide live monthly updates on progress, outputs, milestones and KPIs.

PART 3 – DOCUMENT SUPPORT

Context documents

GLOSSARY

Term	Definition
PPfO	People Portfolio Office (within DPT)
POL	Microsoft Project Online P3M Software tool
PBi	PowerBI (Business Intelligence) Application
BaU	Business as Usual
BP	Business Plan
CDP	Chief of Defence People
DPT	Defence People Team
ExCO	Executive Committee (Defence level Board)
M.Bd	Management Board (CDP internal SLT Board)
P3M	Portfolio, Programme, and Project Management
PftW	Project for the Web
PLT	People Leadership Team
TLB	Top Level Budget
UIN	Unique Identification Number
DAT	Digital Approvals Tool
CP&F	Contracting, Purchasing and Finance
FLC	Front Line Command
SQEP	Suitably Qualified and Experienced Personnel
sS	Single Services
PB&F	Planning, Budgeting and Forecasting
CSA	Control Self Assessment
GOST	Government Online Skills Tool
PMRS	Portfolio Management and Reporting System

CONTRACT MANAGEMENT

1a. The Authority intends to apply Level 1 Standard for contract management to this contract, Level 1 is a 'light touch' approach which might typically be used for contracts below £10m.

1b. The contract manager will have undertaken their contract management foundation course.

1c. Contract Management is the proactive monitoring, control, and management of all activities necessary to ensure the goods, services and works are delivered in accordance with the contractual arrangement.

1d. Where the Contractor is not meeting their obligations, remedies available under the contract will be considered. Effective management of the Authority's contract obligations are of equal importance to the monitoring of a contractor's performance. Therefore, the contract will be proactively managed to ensure that the three core areas of Contract Management, namely Managing Performance & Service Delivery, Contract Administration and Managing Relationships are adhered to.

Key Commercial Activities in Contract Management are:

- a. ensuring the MoD delivers its obligations to the contractor;
- b. issuing any letters to the contractor regarding failure of performance;
- c. ensuring any contract remedies for performance failures are applied promptly
- d. authorising any performance incentives contained in the contract;
- e. ensuring contractors are paid promptly on satisfactory delivery or performance in accordance with the contract payment mechanism;
- f. where there is a formal acceptance process, formally accepting a contractor has performed and delivered their contractual obligations;
- g. Ensuring contract administration and final closure activities are carried out promptly, and in line with policy.

MONITORING PERFORMANCE & PROGRESS MEETINGS

2a. The Contractor shall be responsible for monitoring performance of the deliverables in accordance with the performance criteria set down in the Statement of Requirements, and shall provide the Designated Officer with full particulars, of any aspects of its performance which materially fail to meet the requirements of the Contract, unless otherwise notified in writing by the Authority.

2b. The Contractor shall, consider all requirements arising from the Contract, issue appropriate operating and procedural instructions in writing to their own staff engaged on the Contract.

2c. The Contractor shall maintain such records in respect of the Contract as the Authority may require and will on request produce them for inspection by the Authority. All such records will be kept for 6 years upon Contract expiry or termination, and will not be released, published, or disposed of without the prior written approval of the Authority unless otherwise required by law or regulation.

2d. The Contractor shall, on request by the Designated Officer, make written submissions or oral representations of the work done under the Contract in aid of any review of the performance of the Contract. Review Meetings between the Authority and the Contractor

shall be held as detailed in the Statement of Requirements or as otherwise agreed between the Contractor and the Designated Officer. The Contractor shall make the necessary arrangements for the meetings, which will be held at the offices of the Designated Officer or at the Contractors' premises. A record of all meetings will be made by the Contractor and will be provided to the Authority for its approval no later than 20 working days following the date of the meeting.

2e. The Contractor shall arrange for the attendance of such members of staff and those of their Sub-contractor or agents who may be required by the Authority to attend as witnesses at Boards of Inquiry or similar proceedings.

PERFORMANCE REVIEW PROCEDURES

3. On a quarterly basis after the Contract Commencement Date, the Contractor, DO, Contract Manager and Commercial Manager shall meet to review performance and delivery over the past year in line with the Key Performance Indicators (KPIs) detailed within this document. This review will focus on ensuring the outputs of KPIs are still meeting the requirement and to establish whether there is a need for adjustment. The report will also cover a review of risks and mitigation measures. Any change resulting from this review will be managed in accordance with DEFCON 620 (Edn 06/22) – Contract Change Control Procedure.

ADDITIONAL SERVICES – QUOTATIONS AND AUTHORISATION PROCESS

4a. The Contractor shall submit an estimated resource requirement for the DPT PPfO to review/assessment on the Task Data Form for services required within the Statement of Requirement by the Authority. The Contractor shall not undertake any such work until authorisation has been given by the Authority's Project Manager. Any work undertaken by the Contractor prior to this approval may result in non-payment for this work. The Contractor will then quote the works order number to enable payment

4b. The Contractor shall quote for each Task by completing the form and submitting a copy of the quotation to the Project Team for agreement and authorisation.

4c. Upon authorisation, the Authority shall forward the authorised copy to the contractor to certify the requirement has been completed.

In addition to the terms and conditions of the CCS Framework Agreement RM 1557.10 for G-Cloud 12 the following MOD DEFCONs will apply to any Contract resulting from this Request for Quote.

DEFCON 76 – Contractor's Personnel at Government Establishments

ANNEX B to POL SOR

Dated 28 Feb 23

Original Task No

SUPPLIERS DETAILS

Company Name:

Address:

Registration Number:

NCAGE:

DUNS Number:

Point of Contact:

Name:

Tel:

Email:

COMMERCIAL DETAILS:

Comrc'l Team:

Name:

Tel:

Email:

ANNEX C to POL SOR

Dated 09 Mar 23

PROJECT ONLINE INSTANCE DEVELOPMENT COSTS

ITEM	DESCRIPTION	YEAR 1 Mar 23 to Mar 24	OPTION-YEAR 2 Mar 24 to Mar 25	OPTION-YEAR 3 Mar 25 to Mar 26
1	To satisfy the requirements specified within Statement of Requirement, please provide a price breakdown to include: POL Instance and maintenance, including fixing all bugs and managing change requests Improvement/enhancement to Power BI Reports including further integration across Defence. Management Reporting Function Training Help Function Discovery into the use of Dataverse and PftW		n/a	n/a
2	Support & Development of scheduling and resourcing on any/all of products to be agreed between DPT/PPfO and Defence Commercial by Tasking Form prior to work commencing.	To be costed using person day rates approved by DPT prior to commencement	To be costed using person day rates approved by DPT prior to commencement	To be costed using person day rates approved by DPT prior to commencement
3	Provision of firm person day rate card (by grade) to undertake developments to the system as pre-defined and tasked by the Designated Officer in support of Item 1 Grades of potential work team and Rates: Software Developer Software Tester Software Project Manager		n/a	n/a

Schedule 2: Call-Off Contract charges – Pricing Schedule

ITEM	DESCRIPTION	YEAR 1 Mar 23 to Mar 24	OPTION-YEAR 2 Mar 24 to Mar 25	OPTION-YEAR 3 Mar 25 to Mar 26
1	To satisfy the requirements specified within Statement of Requirement, please provide a price breakdown to include: POL Instance and maintenance, including fixing all bugs and managing change requests Improvement/enhancement to Power BI Reports including further integration across Defence. Management Reporting Function Training Help Function Discovery into the use of Dataverse and PftW	As per section 3, redacted	n/a	n/a
2	Support & Development of scheduling and resourcing on any/all of products to be agreed between DPT/PPfO and Defence Commercial by Tasking Form prior to work commencing.	To be costed using person day rates approved by DPT prior to commencement	To be costed using person day rates approved by DPT prior to commencement	To be costed using person day rates approved by DPT prior to commencement
ITEM	DESCRIPTION	YEAR 1 Mar 23 to Mar 24	OPTION-YEAR 2 Mar 24 to Mar 25	OPTION-YEAR 3 Mar 25 to Mar 26

3	Provision of firm person day rate card (by grade) to undertake developments to the system as pre-defined and tasked by the Designated Officer in support of Item 1 Grades of potential work team and Rates: Software Developer Software Tester Software Project Manager	redacted	n/a	n/a
---	---	----------	-----	-----

Schedule 3: Collaboration agreement – Not applicable

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

Clauses: 2.1 The Customer may, in the Order Form, request the following alternative

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

Clauses: 2.2 2.1.6 References to "tort" will be replaced with "delict" throughout
The Customer may, in the Order Form, request the following Alternative

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988

- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004 • Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

- a. persons of different religious beliefs or political opinions
- b. men and women or married and unmarried persons
- c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
- d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
- e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
- f. persons of different ages
- g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in

accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

- a. the issue of written instructions to staff and other relevant persons
- b. the appointment or designation of a senior manager with responsibility for equal opportunities
- c. training of all staff and other relevant persons in equal opportunities and harassment matters
- d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

- A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its

Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

- 2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.
- 2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

- 2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.
- 2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.
- 2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.
- 2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.
- 2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

- 2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

- 2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.
- 2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.
- 2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

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	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
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	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
Data Loss Event	<p>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.</p>

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	<p>Default is any:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
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-to-date 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	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • 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 <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • 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	<p>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).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.13 together with the Framework Schedules.</p>

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	<p>Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.</p>
Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • 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	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • 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	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>

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	<p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ 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	<p>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.</p>
Property	<p>Assets and property including technical infrastructure, IPRs and equipment.</p>

Protective Measures	<p>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.</p>
PSN or Public Services Network	<p>The Public Services Network (PSN) is the government's highperformance network which helps public sector organisations work together, reduce duplication and share resources.</p>
Regulatory body or bodies	<p>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.</p>
Relevant person	<p>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.</p>
Relevant Transfer	<p>A transfer of employment to which the employment regulations applies.</p>

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 GCloud 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-controlscheck-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 GCloud 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

As per DEFCON 532A (Edn 05/22) - Protection of Personal Data where Personal Data is not being processed on behalf of the Authority

Annex A. The project specific DEFCONs that apply to this Contract

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

However, the Authority call up these additional DEFCONs and in the event of any conflict between them and the RM1557,13 Terms & Conditions, the latter will take precedence.

DEFCON 76

DEFCON 76 (Edn. 11/22) – Contractor`s Personnel at Government Establishments

DEFCON 503

DEFCON 503 (Edn. 06/22) - Formal Amendments To Contract

DEFCON 514

DEFCON 514 (Edn. 8/15) – Material Breach

DEFCON 522

DEFCON 522 (Edn. 11/21) - Payment and Recovery of Sums Due

DEFCON 531

DEFCON 531 (Edn. 09/21) - Disclosure of Information

DEFCON 534

DEFCON 534 (Edn. 06/21) - Subcontracting and Prompt Payment

DEFCON 532A

DEFCON 532A (Edn 05/22) - Protection of Personal Data where Personal Data is not being processed on behalf of the Authority

DEFCON 566

DEFCON 566 (Edn. 12/18) - Change of Control of Contractor

DEFCON 611

DEFCON 611 (Edn. 12/22) – Issued Property

DEFCON 620

DEFCON 620 (Edn. 06/22) - Contract Change Control Procedure

DEFCON 630

DEFCON 630 (Edn. 02/18) - Framework Agreements

DEFCON 632

DEFCON 632 (Edn. 11/21) - Third Party Intellectual Property - Rights and Restrictions

DEFCON 660

DEFCON 660 (Edn. 12/15) - Official-Sensitive Security Requirements

NOTE

1. Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Internet Site:

<https://www.kid.mod.uk/maincontent/business/commercial/index.htm>

2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section off DEFFORM 111.

Annex B - Security Aspects Letter

Date of Issue: 22/03/2023

For the attention of:

Corporate Project Solutions Limited
Jubilee House
Third Avenue
Marlow
Bucks
SL7 1EY



Ministry
of Defence

Main Building, Whitehall,
London SW1A 2H

ITT/CONTRACT NUMBER & TITLE: 707087450 for External Assistance to maintain Project Online (POL) Instance and automated reports using MS PowerBI within Defence People Team (DPT) through G-Cloud 13 Framework Agreement (RM1557.13).

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.
2. Aspects that constitute OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition (annex to this letter) outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
redacted	OFFICIAL-SENSITIVE - Commercial
redacted	OFFICIAL-SENSITIVE
redacted	OFFICIAL-SENSITIVE

(Note: Add more rows as required)

3. Your attention is drawn to the provisions of the Official Secrets Act 1911-1989 in general, and specifically to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989). In particular you should take all reasonable steps to make sure that all individuals employed on any work in connection with this Contract have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply after completion or earlier termination of the contract
4. Will you please confirm that:
 - a. This definition of the classified aspects of the referenced Contract has been brought to the attention of the person directly responsible for security of classified material.

b. The definition is fully understood.

c. Measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. [The requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations.]

d. All employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this contract.

5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

6. Classified Information associated with this Contract must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

7. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76.

Yours
faithfully

Copy via email
to:

[ISAC-Group \(MULTIUSER\)](#)

[COO-DSR-IIPCSy \(MULTIUSER\)](#)

[UKStratComDD-CyDR-CySAAS-021](#)

Annex to Security Aspects Letter

Official and Official-Sensitive Contractual Security Conditions

UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

Purpose

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: COO-DSR-IIPCSy@mod.gov.uk).

Definitions

2. The term "*Authority*" for the purposes of this Annex means the HMG Contracting Authority.

3. The term "*Classified Material*" for the purposes of this Annex means classified information and assets.

Security Grading

4. The SENSITIVE caveat is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading. The Contractor is not required to mark documents graded UK OFFICIAL unless they are transmitted overseas or generated by a Contractor based outside the UK in a third-party country.

Security Conditions

5. The Contractor shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Contractor shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract. The Authority must state the data retention periods to allow the Contractor to produce a data management policy. If you are a Contractor located in the UK your attention is also drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular.

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material

6. The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

7. Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to comply with the accreditation requirements specified in ISNs, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

<https://www.gov.uk/government/publications/industry-security-notices-isns>.

<http://dstan.gateway.isg-r.r.mil.uk/standards/defstans/05/138/000002000.pdf>

<https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down>

8. All UK classified material including documents, media and other assets must be physically secured to prevent unauthorised access. When not in use UK classified material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be controlled.

9. Disclosure of UK classified material must be strictly controlled in accordance with the *"need to know"* principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or sub-Contractor.

10. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any classified material issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 8 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.

11. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.

12. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 34.

Access

13. Access to UK classified material shall be confined to those individuals who have a *"need-to-know"*, have been made aware of the requirement to protect the material and whose access is essential for the purpose of their duties.

14. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE material have undergone basic recruitment checks. This should include

establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf

Hard Copy Distribution

15. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed internally and externally of Contractor premises. To maintain confidentiality, integrity and availability, distribution is to be controlled such that access to documents is only by authorised personnel. They may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

16. Advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE shall be sought from the Authority.

Electronic Communication and Telephony and Facsimile Services

17. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation are available at:

<https://www.ncsc.gov.uk/guidance/tls-external-facing-services>

Details of the CPA scheme are available at:

<https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa>

18. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the information.

19. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-

SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so.

20. UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

Use of Information Systems

21. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

22. The Contractor should ensure **10 Steps to Cyber Security** (Link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure competent personnel apply 10 Steps to Cyber Security.

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.

23. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

24. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK OFFICIAL-SENSITIVE information on IT systems.

a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “*least privilege*” will be applied to System Administrators. Users of the IT System (Administrators) should not conduct ‘standard’ User functions using their privileged accounts.

b. Identification and Authentication (ID&A). All systems are to have the following functionality:

- (1). Up-to-date lists of authorised users.
- (2). Positive identification of all users at the start of each processing session.

c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be “*strong*” using an appropriate method to achieve this, e.g. including numeric and “*special*” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 17 above.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1). The following events shall always be recorded:

- (a) All log on attempts whether successful or failed,
- (b) Log off (including time out where applicable),
- (c) The creation, deletion or alteration of access rights and privileges,
- (d) The creation, deletion or alteration of passwords.

(2). For each of the events listed above, the following information is to be recorded:

- (a) Type of event,
- (b) User ID,
- (c) Date & Time,
- (d) Device ID.

The accounting records are to have a facility to provide the System Manager with a hard copy of all or selected activity. There also must be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this then the equipment must be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability. The following supporting measures are to be implemented:

- (1). Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations),
- (2). Defined Business Contingency Plan,
- (3). Data backup with local storage,
- (4). Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software),
- (5). Operating systems, applications and firmware should be supported,
- (6). Patching of Operating Systems and Applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

h. Logon Banners. Wherever possible, a “*Logon Banner*” will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be:

“Unauthorised access to this computer system may constitute a criminal offence”

i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections. Computer systems must not be connected direct to the Internet or “*un-trusted*” systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).

k. Disposal. Before IT storage media (e.g. disks) are disposed of, an erasure product must be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Laptops

25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 17 above.

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites⁸. For the avoidance of doubt the term “*drives*” includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

27. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

28. Portable CIS devices holding the Authorities’ data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

29. The Contractor shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes MOD Identifiable Information (MODDII) (as defined in ISN2016/05) and any information or asset that has been given a security classification by the UK MOD. The term also includes classified information and assets held by UK Defence Contractors which are owned by a third party e.g. NATO or a another country for which the UK MOD is responsible.

30. In addition any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and

⁸ Secure Sites are defined as either Government premises or a secured office on the contractor premises.

Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD Defence Industry WARP will also advise the Contractor what further action is required to be undertaken.

UK MOD Defence Industry WARP Contact Details

Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)

RLI Email: defencewarp@modnet.r.mil.uk (MULTIUSER)

Telephone (Office hours): +44 (0) 30 6770 2185

Mail: Defence Industry WARP, DE&S PSyA Office
MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

31. Reporting instructions for any security incidents involving Defence Related Classified Material can be found in the Incident Reporting Industry Security Notice at:

<https://www.gov.uk/government/publications/industry-security-notices-isns>

Sub-Contracts

32. Where the Contractor wishes to sub-contract any elements of a Contract to sub-Contractors within its own country or to Contractors located in the UK such sub-contracts will be notified to the Contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.

33. The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a sub-Contractor facility located in another (third party) country. The first page of Annex A (MOD Form 1686 (F1686) of ISN 2022/08 is to be used for seeking such approval. The MOD Form 1686 can be found at:

[ISN 2022-08 Subcontracting or Collaborating on Classified MOD Programmes.pdf \(publishing.service.gov.uk\)](#)

34. If the sub-contract is approved, the Contractor shall flow down the Security Conditions in line with paragraph 32 above to the sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Physical Destruction

34. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when the classified material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE classified material which cannot be destroyed in such a way shall be returned to the Authority.

Private Venture Activities

35. Private Venture (PV) funded (i.e., non-MOD funded) defence related projects and technology fall within one of the following three categories:

- Variants. Variants of standard defence equipment under research, development or in production, e.g., aircraft, military vehicles or ships, etc. with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of an item in-Service with UK Armed Forces;
- Derivatives. Equipment for military or civil use that is not based on standard Service designs but is dependent upon expertise or technology acquired in the course of defence contracts;
- Freelance. Equipment of defence importance that is in no way based on information gained from defence contracts;

36. UK Contractors shall ensure that any PV activity that falls into one of the above categories has been formally security graded by the MOD Directorate of Security and Resilience. Please see PV guidance on the following website further information:

<https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets>

Publicity Material

37. Contractors wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government.

38. For UK Contractors where the exhibition assets relate to multiple Delivery Teams or for Private Venture defence related material where there is no defined Delivery Team, the Contractor shall request clearance for exhibition from the Directorate of Security and Resilience when it concerns Defence Related Material. See the MOD Exhibition Guidance on the following website for further information:

<https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets>

Export sales/promotion

39. The MOD Form 680 (F680) security procedure enables HMG to control when, how, and if defence related classified material is released by UK Contractors to foreign entities for the purposes of promotion or sales of equipment or services. Before undertaking any targeted promotion or demonstration or entering into any contractual commitments involving the sale or release of defence equipment, information or technology classified

UK OFFICIAL-SENSITIVE or above to a foreign entity, a UK Contractor shall obtain F680 approval from the Export Control Joint Unit (ECJU) MOD Team. This includes assets classified UK OFFICIAL-SENSITIVE or above either developed to meet a UK MOD requirement or Private Venture (PV) equipment, as formally advised in a Security Aspects Letter (SAL) issued by the relevant Contracting Authority, or PV Security Grading issued by the MOD Directorate of Security and Resilience. Guidance regarding the F680 procedure issued by ECJU can be found at:

<https://www.gov.uk/government/publications/ministry-of-defence-form-680-procedure-guidance>

40. If a Contractor has received an approval to sub-contract, under an MOD Form 1686 (F1686), for development/production of parts of an equipment, that approval also permits the production of additional quantities for supply to an export customer, when the Contractor has MOD Form 680 approval for supply of the complete equipment, as long as:

- a) they are identical, except for component obsolescence, to items produced under the UK programme that the approval to subcontract relates to; and
- b) no additional OFFICIAL-SENSITIVE or above material is required to be released to the overseas subcontractor.

Interpretation/Guidance

41. Advice regarding the interpretation of the above requirements should be sought from the Authority.

42. Further requirements, advice and guidance for the protection of UK classified material at the level of UK OFFICIAL and UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

<https://www.gov.uk/government/publications/industry-security-notices-isns>

Audit

43. Where considered necessary by the Authority the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractor's processes and facilities by representatives of the Contractor's National/Designated Security Authorities or the Authority to ensure compliance with these requirements.

Annex C. DEFFORM 111

DEFFORM 111 - Addresses and Other Information

1. Commercial Officer

Name: Flavia Fanchin Moedinger

Address: Main Building, Whitehall, London SW1A 2HB

Email: flaviafanchin.moedinger100@mod.gov.uk ☎☎ 03001 58 5676

2. Project Manager, Equipment Support Manager or PT Leader (from whom technical information is available)

Name: Zoe Restall

Address MOD Main Building

Email: Zoe.Restall823@mod.uk ☎☎ 03001653477

3. Packaging Design Authority Organisation & point of contact:

not applicable

(Where no address is shown please contact the Project Team in Box 2)

☎☎ not applicable

4. (a) Supply / Support Management Branch or Order Manager:

Branch/Name: not applicable

☎☎ People Portfolio

(b) U.I.N. People Portfolio

5. Drawings/Specifications are available from not applicable

6. Intentionally Blank

7. Quality Assurance Representative: Zoe Restall

Commercial staff are reminded that all Quality Assurance requirements should be listed under the General Contract Conditions.

8. **AQAPS** and **DEF STANs** are available from UK Defence Standardization, for access to the documents and details of the helpdesk visit <http://dstan.uwh.diif.r.mil.uk/> [intranet] or <https://www.dstan.mod.uk/> [extranet, registration needed].

9. Consignment Instructions The items are to be consigned as follows: not applicable

10. Transport. The appropriate Ministry of Defence Transport Offices are:

A. DSCOM, DE&S, DSCOM, MoD Abbey Wood, Cedar 3c, Mail Point 3351, BRISTOL BS34 8JH

Air Freight Centre

IMPORTS ☎☎ 030 679 81113 / 81114 Fax 0117 913 8943

EXPORTS ☎☎ 030 679 81113 / 81114 Fax 0117 913 8943

Surface Freight Centre

IMPORTS ☎☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946

EXPORTS ☎☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946

B.JSCS

JSCS Helpdesk No. 01869 256052 (select option 2, then option 3)

JSCS Fax No. 01869 256837

www.freightcollection.com

11. The Invoice Paying Authority

Ministry of Defence, DBS Finance, Walker House, Exchange Flags Liverpool, L2 3YL
☎ 0151-242-2000 Fax: 0151-242-2809

Website is: <https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#invoice-processing>

12. Forms and Documentation are available through *:

Ministry of Defence, Forms and Pubs Commodity Management PO Box 2, Building C16, C Site, Lower Arncott, Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)

Applications via fax or email: Leidos-FormsPublications@teamleidos.mod.uk

* NOTE

1. Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Internet Site:
<https://www.kid.mod.uk/maincontent/business/commercial/index.htm>

2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.