Crown Commercial Service

# G-Cloud 12 Call-Off Contract

## Defence Equipment & Support (DE&S) Airworthiness Issues Management System (AIMS) [REDACTED]

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:


*G-Cloud 12 Call-Off Contract* ..... *1*

Part A: Order Form ..... 2

Schedule 1: Services ..... 12

Schedule 2: Call-Off Contract charges ..... 23

Part B: Terms and conditions ..... 25

Schedule 3: Collaboration agreement ..... 44

Schedule 4: Alternative clauses ..... 45

Schedule 5: Guarantee ..... 46

Schedule 6: Glossary and interpretations ..... 47

Schedule 7: GDPR Information ..... 64

Appendix 1 – Service Levels, Service Level Agreements and Service Credits ..... 66

Appendix 2 - Implementation Plan ..... 67

Appendix 3 – Exit Strategy ..... 68

Appendix 4 – Training Plan ..... 69

Appendix 5 – User Access Control ..... 70

Appendix 6 – Business Continuity and Disaster Recovery ..... 71

Appendix 7 – Additional Tasking Process ..... 72

Appendix 8 – Security Aspect Letter ..... 80

# 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.

| | |
|---|---|
| **Digital Marketplace service ID number** | 9222 4897 6322 427 |
| **Call-Off Contract reference** | 703454451 DCT002 |
| **Call-Off Contract title** | DE&S Interim Airworthiness Issues Management System |
| **Call-Off Contract description** | DE&S Interim Airworthiness Issues Management System (AIMS) |
| **Effective Contract Start date** | 01 April 2023 |
| **Contract Expiry date** | 31 March 2025 |
| **Call-Off Contract value Maximum Price** | £9,119,520.00 |
| **Charging method** | Payment shall be made by the Buyer's e-payment system "CP&F" (via Exostar) |
| **Purchase order number** | TBC |

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

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

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

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

| | |
|---|---|
| **From the Buyer** | Defence Equipment and Support<br>030 679 34324<br>MoD Abbey Wood<br>Spruce 2B #1261<br>Bristol<br>BS34 8JH |
| **To the Supplier** | TLMNEXUS Limited<br>0845 677 4480<br>Telecom House<br>125-135 Preston Road<br>Brighton<br>East Sussex<br>BN1 6AF<br>United Kingdom<br>Company number: 04058701 |
| **Together the 'Parties'** | |

## Principal contact details

**For the Buyer:**

Title: Commercial Officer

Name: Ryan Miller

Email: [REDACTED]

Phone: [REDACTED]

**For the Supplier:**

Title: Commercial Director

Name: Anthony Harris

Email: [REDACTED]

Phone: [REDACTED]

## Call-Off Contract term

| | |
|---|---|
| **Start date** | This Call-Off Contract Starts on 01 April 2023 and is valid until 31 March 2025.<br><br>The date and number of days or months is subject to clause 1.2 in Part B below. |
| **Ending (termination)** | The notice period for the Supplier needed for Ending the Call-Off Contract is at least **40** Working Days from the date of written notice for undisputed sums (as per clause 18.6).<br><br>The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1). |
| **Extension period** | This Call-off Contract can be extended by the Buyer for **2** periods of 12 months, by giving the Supplier **12 weeks** written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.<br><br>The Call-off Contract may be extended in full (all platforms as identified in the Call-off Contract Charges) or in part by the Buyer specifying the platforms to be included at the point of extension.<br><br>Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.<br><br>The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each.<br><br>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: |

| | |
|---|---|
| | https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service |

## Buyer contractual details

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

| | |
|---|---|
| **G-Cloud lot** | This Call-Off Contract is for the provision of Services under:<br>• Lot 2: Cloud software |
| **G-Cloud services required** | The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:<br><br>Cloud software Services sold through G-Cloud are applications that are accessed over the internet and hosted in the cloud.<br><br>The G-Cloud cloud software Lot is equivalent to the National Institute of Standards and Technology definition of 'Software as a Service'.<br><br>1.1.1 Collaborative Working<br>1.1.2 Electronic document and records management (EDRM)<br>1.1.3 Information and communication technology (ICT)<br>1.1.4 Operations Management<br>1.1.5 Software development tools |
| **Additional Services** | The Supplier shall provide additional DE&S Airworthiness Issue Management Services in accordance with an Additional Tasking Process. The scope of that work includes:<br><br>- Interface and data uploading services;<br>- Configuration services;<br>- Training services including face-to-face and tailored training materials,<br>- Data migration services;<br>- Data archiving services;<br>- Technical subject matter expertise; |

| | |
|---|---|
| | MoD Data processing activities (this shall include the need for Supplier employees shall sign a DEFFORM 702 (Employee's Acknowledgement to Employer of Obligations Relating to Confidentiality) where any MoD data will need to be processed) |
| **Location** | The Services will be delivered to DE&S Delivery Teams supporting Air Platforms.<br><br>Unless otherwise agreed by the Parties, the Services will be delivered to Defence Equipment and Support, MoD Abbey Wood, Bristol, BS34 8JH. |
| **Quality standards** | The quality standards required for this Call-Off Contract are in accordance with the Supplier's G-Cloud 12 Cloud Software Service Definition Document. |
| **Technical standards:** | The technical standards used as a requirement for this Call-Off Contract are in accordance with the Supplier's G-Cloud 12 Software Service Definition Document. |
| **Service level agreement:** | The service level and availability criteria required for this Call-Off Contract are in accordance with Appendix 1 – Service Level Agreement. |
| **Onboarding** | The onboarding required for this Call-Off Contract is in accordance with Appendix 2 - Implementation Plan.<br><br>Should the Buyer identify a requirement to onboard additional Platforms / Delivery Teams, the Buyer will issue a Request for Quote to the Supplier. The Supplier's quote as a minimum may include charges for Configuration, Onboarding and the monthly charges in accordance with Schedule 2. Should the Buyer which to proceed with the Platform / Delivery Team onboarding, the configuration and onboarding will be in accordance with the Appendix 7 Additional Tasking Process and the monthly charges will form an amendment to Schedule 2. |
| **Offboarding** | In accordance with Appendix 3 – Exit Strategy.<br><br>During the Term the Buyer may offboard Platform / Delivery Teams as required by providing the Supplier with two weeks' notice. The Call-Off Contract Charges detailed in the tables below are the Total Maximum Price. The Supplier will only |

| | |
|---|---|
| | charge the Buyer for Platforms / Delivery Teams which have not been offboarded and are using the DE&S Airworthiness Issues Management System (RESOLVE) tool on a monthly basis. |
| **Collaboration agreement** | Not Applicable. |
| **Limit on Parties' liability** | [REDACTED] |
| **Insurance** | • [REDACTED] |
| **Force majeure** | A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 15 consecutive days. |
| **Audit** | The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits in accordance with clauses 7.4 to 7.13 of the Framework Agreement. |

| | |
|---|---|
| **Buyer's responsibilities** | The Buyer is responsible for granting access to MOD Establishments / Locations and / or MODNet if access is required and agreed by the Buyer in order for the Supplier to fulfil their obligations under this Call-off Contract. |
| **Buyer's equipment** | The Buyer's equipment to be used with this Call-Off Contract will be agreed between the Parties as required during the period of this Call-off Contract. |

## Supplier's information

| | |
|---|---|
| **Subcontractors or partners** | The following is a list of the Supplier's Subcontractors or Partners**:**<br><br>**Devonport Royal Dockyard Limited** |

## 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 the Buyer's e-payment "CP&F" (Contracting, Purchasing & Finance) system in accordance with the following conditions where "Contractor" shall mean the Supplier and "Authority" shall mean the Buyer:<br><br>DEFCON 5J<br><br>DEFCON 129J<br><br>DEFCON 522 |
| **Payment profile** | The payment profile for this Call-Off Contract is **monthly** in arrears. |
| **Invoice details** | The Supplier will issue electronic invoices in accordance with the Payment Method. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice. |

| | |
|---|---|
| **Who and where to send invoices to** | Invoices will be sent via Exostar in accordance with the Payment Method detailed above. |
| **Invoice information required** | All invoices must include the project reference 703454451. |
| **Invoice frequency** | Invoice will be sent to the Buyer in accordance with the Call-Off Contract charges. |
| **Call-Off Contract value Maximum Price** | The total maximum value of this Call-Off Contract is £9,119,520.00. |
| **Call-Off Contract charges** | The breakdown of the Charges is in accordance with Schedule 2 – Call-off Contract charges. |

## Additional Buyer terms

| | |
|---|---|
| **Performance of the Service and Deliverables** | In accordance with Appendix 1 – Service Level Agreement, Appendix 2 - Implementation Plan and Appendix 3 – Exit Strategy. |
| **Guarantee** | Not Applicable. |
| **Warranties, representations** | In accordance with Framework Agreement clause 4.1. |
| **Supplemental requirements in addition to the Call-Off terms** | Not Applicable. |
| **Alternative clauses** | Not Applicable. |
| **Buyer specific amendments to/refinements of the Call-Off Contract terms** | Within the scope of the Call-Off Contract, the Supplier agrees to the following conditions where “Contractor” shall mean the Supplier and “Authority” shall mean the Buyer:<br><br>DEFCON 76 – 06/21 - Contractor's Personnel at Government Establishments<br><br>DEFCON 513 – 07/21 - Value Added Tax |

| | |
|---|---|
| | DEFCON 515 – 06/21 - Bankruptcy and Insolvency<br><br>DEFCON 516 – 04/12 - Equality<br><br>DEFCON 522 - 11/21 - Payment and Recovery of Sums Due<br><br>DEFCON 524 – 12/21- Rejection<br><br>DEFCON 525 - 10/98 - Acceptance<br><br>DEFCON 531 – 9/21 - Disclosure of Information<br><br>DEFCON 534 - 06/21 - Subcontracting and Prompt Payment<br><br>DEFCON 611 - 02/16 - Issued Property<br><br>DEFCON 604 - 06/14 - Progress Reports<br><br>DEFCON 608 – 07/21 - Access and Facilities to be Provided by the Contractor<br><br>DEFCON 609 – 07/21 - Contractor's Records<br><br>DEFCON 625 – 06/21 - Co-operation on Expiry of the Contract<br><br>DEFCON 637 - 05/17 - Defect Investigation and Liability<br><br>DEFCON 642 – 07/21 - Progress Meetings<br><br>DEFCON 658 – 09/21 – Cyber<br><br>Further to DEFCON 658 the Cyber Risk Profile of the Contract is [REDACTED], as defined in Def Stan 05-138.<br><br>DEFCON 660 - 12/15 - Official Sensitive Security Requirements<br><br>DEFCON 695 - 02/15 - Contract Costs Statement Post Costing (Non-qualifying Contract) |
| **Public Services Network (PSN)** | The Public Services Network (PSN) is the government's secure network.<br><br>If the G-Cloud Services are to be delivered over PSN this should be detailed here:<br><br>The services will be delivered in accordance with Schedule 1 - Statement of Requirement. |
| **Personal Data and Data Subjects** | Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1 |

## 1. Formation of contract

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

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

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

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

## 2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.

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

| | | |
|---|---|---|
| **Signed** | Supplier | Buyer |
| **Name** | Anthony Harris | Sarah Mitchell |
| **Title** | Commercial Director | Senior Commercial Manager |
| **Signature** | [REDACTED] | [REDACTED] |
| **Date** | 22/09/2022 | 14/09/2022 |

# Schedule 1: Services

**Part A – DE&S Airworthiness Issues Management software requirement**

| Serial | Requirement |
|---|---|
| **A.1 - Key Software functionality** | |
| A.1.1 | The DES AIMS software shall enable the reporting and management of Airworthiness Issues by Authorised Users. |
| A.1.2 | The DES AIMS software shall facilitate the management of Airworthiness Issues by enabling the undertaking of tasks, decisions and Actions to lead to the resolution of Airworthiness Issues, including linked Processes, as required. |
| A.1.3 | The DES AIMS software shall enable data to be interfaced / exchanged with other MoD and Industry owned airworthiness and business software tools. |
| A.1.4 | The DES AIMS software shall facilitate the sharing of documents between DE&S FAST Delivery Team, Front Line Command and BAEs users (the E-Library requirement at A.4). |
| A.1.5 | The DES Aims software shall store equipment hazards within the system (as imported from eCassandra); |
| A.1.6 | The management of Airworthiness Issues is complex due to interdependencies and wide-span of stakeholders and provides essential support to operational Air Systems and associated equipment. The DES AIMS software shall be able to manage high volumes of complex Airworthiness Issues. |
| A.1.8 | The DES AIMS software shall provide a concurrency of use to meet the DES AIMS Requirement Part B and C. |
| A.1.9 | The DES AIMS software shall provide the ability to flexibly configure Authorised User access controls and permissions. |
| A.1.10 | The DES AIMS software shall provide an audit trail of all Authorised User activity within the system |
| A.1.11 | The DES AIMS software shall provide a full and comprehensive chronological audit trail of decisions and evidence underpinning issues and entities. |
| A.1.12 | The DES AIMS software shall provide the ability to generate a snapshot of all data related to a single Air System, without disrupting day-to-day business, within 1 hour of any given moment. This snapshot shall be an un-editable baseline of the data set in order to deliver credible data to the Defence Air Accident Investigation Board in the event of an accident. |
| **A.2 – Compliance with workflows** | |
| A.2.1 | The software shall provide a workflow to enable the user to conduct the processes described in the following paragraphs |
| A.2.2 | Management/processing of Airworthiness Issues, as described in A3, including linking to respective inputs, outputs and other aspects of airworthiness management enabled within the DES AIMS software. |
| A.2.3 | Management/processing of Airworthiness Issues Management system inputs/outputs<br>- Technical input to Defence Air Safety Occurrence Reports (DASORs) (inter-face with ASIMS)<br>- Significant Engineering Safety Occurrence Reports (SESORs) (interface with ASIMS)<br>- Technical Warnings<br>- Service Bulletins<br>- Special technical orders (investigation)<br>- Special technical orders (change)<br>- Quality Occurrence Reports (QORs)<br>- Operational Occurrence Reports<br>- Reportable Occurrences<br>- Narrative fault (MF760) reporting |

| | |
|---|---|
| | - Air System Document Set (ADS) Unsatisfactory Feature Report (UFR) (MF765 and MF65X)<br>- Technical publication request form<br>- Technical enquiries<br>- Management Activity and Actions, e.g. Service inquiry recommendations<br>- Management/processing of Airworthiness Issues Management system outputs<br>- General messaging<br>- Special Instructions (Technical)<br>- Support policy letters<br>- Leaflet 103E management (Merlin)<br>- Signal amendment<br>- Special flying instructions<br>- In-Service Design Changes<br>- Design Organisation modifications (legacy items)<br>- Service Modifications (legacy items)<br>- Production System Configuration (PSC) lookup table (service modification enabler) |
| A.2.4 | Management/processing of other Type or Continuing Airworthiness functions<br>- Management of equipment hazards<br>- Safety assessment<br>- Air system topic 2 (N/A/R)1 leaflets<br>- Aircraft integrity management data and dashboards<br>- Supplier concessions<br>- Engineering concessions<br>- Leaflet 109D management (Merlin)<br>- Extension requests (lifting and maintenance)<br>- Deviation reports<br>- Aircraft structural health monitoring<br>- Structural zonal inspections (Topic 5V)<br>- Design Organisation repairs 2 (N/A/R)5<br>- Engineering support demand Management<br>- Data change requests<br>- Upload mass properties |
| A.2.5 | The workflow provided shall be in a manner compliant with<br>- the associated MAA Regulatory Publication (MRP) (regulatory article or manual)<br>- DE&S-issued policy (including that contained in the Air Engineers Toolkit (AET) or issued as DG Air Policy Instruction (DGAPI)) and<br>- the AIMS Process Requirements document.<br><br>When there is a conflict between the procedural steps described in these documents, the order of primacy shall be: MRP; DGAPI; AET; AIMS Process Requirements. |
| **A.3 – Software functionality** | |
| A.3.1 | The DES AIMS software shall enable Authorised Users to:<br>- Access the tool via a web front end from a variety of browser types;<br>- Able to be accessed by a MODNet user, via a standard MOD-issue laptop<br>- Originate, process, track and record Issues and / or Entities;<br>- Record details of record, retain and recover details of all Events;<br>- Assign and reassign Issues and / or Entities to another User;<br>- Assign Actions to other Users with User defined timelines, deadlines and priorities;<br>- Complete mandated fields (these shall be defined by the customer as part of system implementation) have been populated; |

| | |
|---|---|
| | - Attach digital Artefacts to Issues and / or Entities and support the following formats:<br>  - Pdf files;<br>  - Photographs/images (at a minimum .bmp, .jpeg and .png);<br>  - Microsoft Office documents.<br>- View and make comments on digital Artefacts attached to Issues and / or Entities;<br>- View a summary of all Actions assigned to them, including deadlines and priorities;<br>- Search the DES AIMS for Issues, Entities; Artefacts and Actions using key words (free text), record ID, Air System & date ranges (at a minimum);<br>- Close or archive an Issue and / or Entity;<br>- Re-open a closed or archived Issue and / or Entity;<br>- Manage items assigned to them as 'work in progress' or draft and noting that these should not be visible to others prior to publication;<br>- Publish 'work in progress' or drafts when completed;<br>- Link the following AIMS elements:<br>  - Artefacts to Issues and / or Entities;<br>  - Hazards to Issues and / or Entities (linkage only as part of the DASOR Entity / Process);<br>  - Issues to Entities and Entities to Issues;<br>  - Issues to Issues.<br>- Record any decision of review, amendment or approval with a time/date stamp;<br>- Provide comments and / or justification for approvals / decisions;<br>- Access chronological audit trail of decisions and evidence underpinning the progression of an Issue;<br>- Print content from within AIMS including:<br>  - Events and linked elements<br>  - Issues and linked elements,<br>  - Entity and linked elements,<br>  - Artefacts,<br>  - Reports;<br>- Print Issues and Entities including in standardised formats as appropriate<br>- Export a single or multiple Issues and / or Entities in pdf format including all related Artefacts, Issues and Entities including in standardised formats as appropriate.<br>- Export a single or multiple Issues and / or Entities in Microsoft Word Document format including all related Artefacts, Issues and Entities including in standardised formats as appropriate.<br>- Export a single or multiple Issues and / or Entities in csv format including all related Artefacts, Issues and Entities.<br>- Export a single or multiple Issues and / or Entities to a SQL database maintaining the relationship between all AIMS elements (Issues, Entities, Artefacts).<br>- Export digital Artefacts in the format they were originally uploaded into AIMS.<br>- Export data from the DES AIMS software in accordance with the AIMS Data Interface Data Dictionaries.<br>- Import data into the DES AIMS software in accordance with the AIMS Data Interface Data Dictionaries.<br>- Export data from the DES AIMS software in accordance with the BAEs PLM and DSE Interface Control Document (ICD) Requirement.<br>- Import data from the DES AIMS software in accordance with the BAEs PLM and DSE Interface Control Document (ICD) Requirement.<br>- Download and print standard reports to review Issue and / or Entity progression, ownership and performance. |

| | |
|---|---|
| A.3.2 | The DES AIMS software shall be based on one consistent logical database structure, including consistent naming conventions and table / entity structures. |
| **A.4 - E-Library functionality for the FAST Delivery Team Users** | |
| A.4.1 | The DES AIMS e-Library shall facilitate, for the FAST Delivery Team Users, the publication of:<br>Special Instructions (Technical) Leaflets<br>Service Modifications Leaflets<br>Service Modification Compatibility Matrix (SMCM)<br>Aircrew Technical Publications (ATPs)<br>Product Software Configuration (PSC) Guidance Document<br>Supporting documentation (where appropriate) |
| A.4.2 | The e-Library shall support the following document formats, .pdf, .doc/docx, .xls/xlsx, .ppt/pptx, .odt, .ods, .odp, .html, .txt, .tif, .jpg, .jpeg, .png, .msg, .zip |
| A.4.3 | The e-library shall display the latest published version of all documents. |
| A.4.4 | The e-Library shall allow FAST Delivery Team Users to access the tool as either READ ONLY, AUTHOR or APPROVER. |
| A.4.5 | The e-Library shall facilitate FAST Delivery Team User Groups to have appropriate access to documentation held in the tool. |
| A.4.6 | FAST Delivery Team Users shall be able to access the e-Library through the DES AIMS portal. |
| A.4.7 | The e-Library shall be accessible via MODNET. |
| A.4.8 | The e-Library shall facilitate the exporting of published documents to suitable media/hardware for non-connected deployments. |
| A.4.9 | Where a compliant format is uploaded, then the e-Library shall publish such documents in the recommended HMG Format. |
| A.4.10 | All e-Library publications shall have an AUTHOR and an APPROVER to enable publication. |
| A.4.11 | All publications the e-Library shall be hold details of:<br>[Serial Number]<br>[Form Type]<br>[Title]<br>[Sponsor]<br>[Created By]<br>[Created Date]<br>[Workflow Assignee]<br>[Status]<br>[Review Date]<br>[RAG Status]. |
| A.4.12 | The e-Library shall facilitate a ‘Review Cycle’ for all manual publications. |
| **A.5 – Dashboards and reporting** | |
| A.5.1 | The software shall allow for Authorised Users with access to standard dashboards and reports to provide management information / metrics at:<br>- Operating centre level, covering multiple Air Systems across multiple delivery teams;<br>- TAA level, covering multiple Air Systems across a single delivery team;<br>- Air system level, covering a single Air System;<br>- Authorised User level (summary of all Actions assigned to an individual, including deadlines and priorities).<br>Such standard dashboards and reports shall include as a minimum at each of these levels:<br>- Issue and Entity progression;<br>- Issue and Entity Ownership;<br>- Issue and Entity Performance. |
| A.5.2 | The software shall provide Authorised Users with access to standard dashboard reports on-screen, downloadable and printable in both Microsoft Word and pdf formats. |

| | |
|---|---|
| A.5.3 | The software shall provide Authorised Users the ability to bulk export system usage and performance data in .csv format to support DE&S's internal management information systems and dashboards. |
| **A.6 – System administration functionality** | |
| A.6.1 | The DES AIMS software shall enable persons assigned to the system administration role to perform routine system administration tasks via appropriate access permissions. Such tasks shall include, but not be limited to:<br>- Use system administration tools to maintain DES AIMS;<br>- Add, change or remove Authorised Users;<br>- Define and Set permission level groups for Authorised Users;<br>- Conduct archiving activities;<br>- Set-up and maintain User look-up lists;<br>- Export bulk data from DES AIMS;<br>- Define, approve and set each Authorised Users permission, authority and access rights. |

**Part B – The DES AIMS implementation requirement**

| Serial | Requirement |
|---|---|
| **B.1 Go-Live** | |
| B.1.1 | The Supplier shall be responsible for providing the DES AIMS software to meet a Go-live date of the 01 April 2023. |
| **B.2 Data Migration** | |
| B.2.1 | The supplier shall create a Data Migration Plan for review and acceptance by the Authority. |
| B.2.2 | The Supplier shall migrate the data from the existing supplier managed software system in accordance with the Data Migration Plan and in line with the DES AIMS Data Migration Extant Position to be supplied by the Authority as required. |
| B.2.3 | The Supplier shall import all historical and archived records (from the existing AIMS solution) from provided data files maintaining all relationships between data elements (this shall include any data previously imported (into the existing AIM tool) from other sources). Details of the data to be migrated will be provided at an agreed date during the implementation of DES AIMS. |
| B.2.4 | The Supplier shall ensure all data integrity is maintained without:<br>- missing data;<br>- losing data; and / or<br>- corrupting data. |
| B.2.5 | The Supplier shall provide validation of the migrated data in accordance with the Data Migration Plan. |
| B.2.6 | The Supplier shall provide full audit documentation for data migration to the Authority. |
| B.2.7 | The Supplier shall conduct initial population of the DES AIMS with all Authorised Users (as identified by the Authority during the implementation of DES AIMS) to enable them to access the system. |
| **B.3 Software and network approval** | |
| B.3.1 | The Supplier shall ensure that DES AIMS conforms to the most recent version of JSP604 Network Joining Rules (an indication of the necessary process for undertaking this is provided within the JSP604 Network Joining Rules Overview in the Data Room). As part of this requirement the Supplier shall provide, at or shortly after contract placement:<br>- a clearly defined high level information exchange document;<br>- a high level network diagram |
| B.3.2 | The Supplier shall manage the DES AIMS software and network accreditation process in accordance with JSP604, DEF STAN 05-138 ISO 27001/2 principles and industry best practice and demonstrate access from MODNET and across the |

| | |
|---|---|
| | Assured LAN Interconnect (ALI). This includes the Supplier undertaking any necessary testing and providing documentation to provide evidence in support of the JSP 604 process to achieve an Interim Authority to Operate by 1st April 2023 |
| B.3.3 | The Supplier shall provide suitable technically qualified subject matter experts to support, JSP 604 Network Joining Rules and ISS approvals process (including Authority to Test, Interim Authority to Operate, Full Authority to Operate and associated accreditation processes) prior to the service going live. |
| B.3.4 | The Supplier shall ensure that the DES AIMS service is available with an appropriate level of concurrency of use and accessible from:<br>- MODNET base and overseas capabilities, utilising both desktop and laptop devices;<br>Industry approved devices operating on the MOD Assured LAN Interconnect (ALI). |
| B.3.5 | The Supplier shall ensure that the DES AIMS service is only accessed by approved devices operating on the official MODNET networks or through the Assured LAN Interconnect (ALI) and use DNS (instead of IP address literals) to identify devices and services wherever possible. |
| B.3.6 | The Supplier shall achieve DES AIMS Browser compatibility with the following browser types and versions:<br>- Internet Explorer browser (current version 1909 [OS Build 18363.2158] and all later versions) contained within the MODNET build (base and overseas);<br>- Chrome browser (version 98.0.4758.102 and all later versions) contained within the MODNET build (base and overseas);<br>- Microsoft Edge browser (current version 99.0.1150.36 and all later versions) contained within the MODNET build (base and overseas); |
| B.3.7 | The Supplier shall achieve DES AIMS Browser compatibility with the following browser types and versions:<br>- Internet Explorer browser (version assumed to be newer than MODNET version) running on Industry owned approved devices operating on the official network (via the Assured LAN Interconnect (ALI));<br>- Chrome browser (version assumed to be newer than MODNET version) running on Industry owned approved devices operating on the official network (via the ALI).<br>- Microsoft Edge browser (version assumed to be newer than MODNET version) running on Industry owned approved devices operating on the official network (via the ALI). |
| B.3.8 | The Supplier shall ensure that the DE&S Airworthiness Issue Management System complies with MOD Domain Name Space Hierarchy and relevant MOD policy leaflets (as per the MoD DNS Policy Leaflet in the Data Room) for all implementations. |
| B.3.9 | The Supplier shall demonstrate compliance with all relevant safety legislation, regulations and standards including as a minimum JSP430, JSP454 and Def Stan 00-56. |
| B.3.10 | The Supplier is responsible for engaging with the appropriate accreditation process to enable the DES AIMS system (including software, infrastructure and hosting environment) to achieve accreditation prior to go-live. |
| B.3.11 | The Supplier shall demonstrate compliance with Cyber Essentials. |
| B.3.12 | The Supplier shall provide a secure backup capability to enable restoration of MoD information in accordance with the Business Continuity and Disaster Recovery Plan at C.5. |
| B.3.13 | The Supplier shall operate, manage and host the DES AIMS service from the UK and in UK based data centre(s) and within the MOD network boundary (most likely within Authority Zone 2a; to be confirmed during the execution of JSP604 processes). |

| | |
|---|---|
| B.3.14 | The Supplier shall operate the DES AIMS service to handle 'Official-Sensitive' data defined in accordance with JSP440 Part 4. |
| B.3.15 | The Supplier shall manage the DES AIMS software and network accreditation process in accordance with JSP604, DEF STAN 05-138 ISO 27001/2 principles and industry best practice and demonstrate access from MODNET, DII and across the Assured LAN Interconnect (ALI). This includes the Supplier undertaking any necessary testing and providing documentation to provide evidence in support of the JSP 604 process to achieve an Authority to Operate no later than 01 April 2023. |
| **B.4 Configuration** | |
| B.4.1 | The Supplier shall create a Configuration Plan for review and acceptance by the Authority. |
| B.4.2 | The Supplier shall provide and configure the DES AIMS software in accordance with the Software Configuration Plan and to ensure compliance with:<br>- MAA Regulations;<br>- Internal DE&S procedures<br>- Air Environment policy; |
| B.4.3 | The Supplier shall conduct testing services on the configured DES AIMS software in accordance with the Software Configuration Plan and to ensure compliance with:<br>- MAA Regulations;<br>- Internal DE&S procedures<br>- Air Environment policy; |
| B.4.4 | The Supplier shall configure and successfully test import and export functionality in accordance with the AIMS Data Interface Data Dictionaries, the specified Interface Control Document (ICD) and the Software Configuration Plan. |
| B.4.5 | The Supplier shall configure and successfully test MOD standardised formats for both printing and exporting data from the DES AIMS software in accordance with the formats provided as part of the process descriptions (per the MRP, the AET, the AIM Process Requirements etc), and in accordance with the Software Configuration Plan. |
| B.4.6 | The Supplier shall identify where the AIM Process Requirements differ from those in the MRP or DE&S Air Environment policy (in particular the current processes in the DE&S Air Engineers Toolkit) and, prior to the implementation phase, shall gain agreement of the Authority on a course of action to close or tolerate any gaps. |
| B.4.7 | The DES AIMS software shall be configured to enable Authorised User Access permissions in accordance with the DES AIMS Access Strategy and the software Configuration Plan. Role permission profiles will be provided by the Authority during the implementation of DES AIMS. |
| **B.5 User Readiness and training** | |
| B.5.1 | The Supplier shall create a Training Plan for review and acceptance by the Authority. |
| B.5.2 | The Supplier's responsibilities shall include provision of initial training, for all Authorised Users in accordance with the Training Plan using appropriate training methods and approaches as necessary to enable Authorised Users to competently operate the DES AIMS software.<br><br>The Supplier shall ensure that Authorised Users have sufficient awareness training to enable them to access and use the service from 01 April 2023 and in accordance with the agreed Training Plan.<br><br>Competence is defined here as the ability to operate the system effectively and efficiently, as appropriate to the individual's role without supervision in accordance with the User and System functionality as specified in this SOR. The Supplier shall tailor training to roles and enable Authorised Users to manage Events, Issues and Entities without supervision. |

| | |
|---|---|
| | The Suppliers training methods shall include (but not be limited to):<br>- online training in accordance with UK Government Assisted Digital Guidance and accredited where required within the Government Digital by Default Services Standard and accessible from the MoD Network and end user devices (**Note: Online training will need to be tested and authorised for access across the MoD Networks**);<br>- Integrated user guides both for Authorised Users and Authorised Users in the system administration role include supporting on screen prompts;<br>- Provision of SCORM training packages for DE&S to host and utilise for training of Authorised Users;<br>- face to face training. |
| B.5.3 | A minimum of 25% of Authorised Users (as specified by the Authority prior to commencement of the training) shall be competent (trained) to operate the system by 01 April 2023. |
| B.5.4 | The Supplier shall ensure that the remaining Authorised Users have sufficient awareness and / or training to enable them to access and use the service by 01 October 2023 and in accordance with the agreed Training Plan. |
| B.5.5 | The Supplier shall include in their Training Plan the requirement for New User and top training as per Part C.8 – New User and top-up training. |

**Part C – The DES AIMS service requirement**

| Serial | Requirement |
|---|---|
| **C.1 – Service** | |
| C.1.1 | The Supplier shall provide a fully accredited DES AIMS service as a managed application service with access from MoD accredited, network attached, devices in accordance with JSP 604, DEF STAN 05-138, ISO 27001/2 principles and industry best practice. This includes the provision of suitable, technically qualified subject matter experts to maintain accreditation over the life of the contract. |
| C.1.2 | The Supplier shall ensure that the software functionality is adapted as necessary to allow the user to remain compliant with all relevant MAA Regulations and DE&S Air Environment policy/processes. |
| C.1.3 | The Supplier shall not access data held on DES AIMS in the operation of the DES AIMS service provision but shall enable Authorised Users to access and handle data held on DES AIMS. |
| C.1.4 | The supplier shall ensure that all data (including archived material) is accessible 24/7 365 days per year to all Authorised Users |
| **C.2 – Technical support** | |
| C.2.1 | The Supplier shall provide a DES AIMS support helpdesk for all Authorised Users between the hours of 9am and 5pm in accordance with the SLA, Monday to Friday (excluding Bank Holidays) via telephone. |
| C.2.2 | The Supplier shall provide an online support facility on 24/7 basis which as a minimum allows Authorised Users to raise incidents, obtain information on major outages and on planned maintenance. |
| C.2.3 | The Supplier shall provide a Single Point of Contact (SPoC). |
| C.2.4 | The Supplier shall provide technical support to resolve service incidents, problems and requests (terms as defined by ITIL) on a 24/7 basis. |
| C.2.5 | The Supplier shall provide all levels of technical application and infrastructure support (1st, 2nd, 3rd line) |
| C.2.6 | The Supplier shall apply Information Technology Infrastructure Library (ITIL) best practices, including incident, problem and change management to minimize the risk of recurring problems and negative Authorised User impacts. |
| **C.3 - Service levels** | |

| | |
|---|---|
| C.3.1 | The Supplier shall produce a Service Level Agreement (SLA) for agreement by the Authority during the Implementation Phase. The SLA shall capture the service levels and other performance criteria set out in these Requirements, such as may need to be referred to by Authorised Users or by the Authority in the day to day management of the Service. The Supplier may amend the draft SLA provided by the Authority for this purpose. |
| C.3.2 | The Supplier shall provide the service on a 24 hour basis, 365 days-a-year. The supplier shall propose in the SLA a means of measuring Availability for all Authorised Users at the agreed concurrency of use. Availability here shall be defined as full functionality of the toolset being available to all Authorised Users, in all locations at agreed performance levels. |
| C.3.3 | The Supplier shall propose in the SLA a minimum performance level, meaning here the ability to access and use DES AIMS and bound by any agreed constraints (such as concurrent Users and boundaries of responsibility) where the level is consistent with reasonable expectations of business usage of the service and in accordance with the User Journeys; |
| C.3.4 | The Supplier shall propose in the SLA incident resolution times. |
| C.3.5 | The Supplier shall use active system monitoring and alerting for service availability, infrastructure, data replication and security breaches (at a minimum). |
| C.3.6 | The Supplier shall provide and maintain the DES AIMS service in accordance with the SLA. |
| C.3.7 | The Supplier shall maintain User access control. |
| **C.4 - System Administration Support** | |
| C.4.1 | The Supplier shall provide full system administration support services covering all system administration activities to all Authorised Users.as detailed in A.6.1. |
| C.4.2 | The Supplier shall monitor and report performance of the system administration support service, described in the System Administration section in the Service Level Agreement. |
| C.4.3 | The Supplier shall be able to scale the DES AIMS system administration support services up or down. |
| **C.5 - Business Continuity and Disaster Recovery** | |
| C.5.1 | The Supplier shall create and maintain a Business Continuity and Disaster Recovery Plan and make this available for review by the Authority throughout the life of the contract. |
| C.5.2 | The Supplier shall conduct and report against at least one successful disaster recovery simulation every Contract Year, against the stated RPO and RTO, described in the Business Continuity and Disaster Recovery Plan. |
| C.5.3 | The Supplier shall provide business continuity and disaster recovery services based upon:<br>- A Recovery Point Objective (RPO) of 12 hours (100% of service capability and data recovered) applying to the point at which incident or loss occurs;<br>- A Recovery Time Objective (RTO) of 24 hours or 7 working hours (whichever is lesser) to restore to the agreed RPO or better. |
| C.5.4 | The Supplier shall maintain a disaster recovery capability sufficient to restore the DES AIMS service to the RPO within the stated RTO. |
| C.5.5 | The Supplier shall invoke the disaster recovery capability when requested by the Authorities named POCs. |
| C.5.6 | The Supplier shall maintain the capability to securely backup information and enable its restoration in the event of business interruptions or disasters including security related incidents and data protection breaches. |
| C.5.7 | The DES AIMS service shall receive:<br>- critical security patches within two weeks;<br>- non-critical security patches at a minimum of every six months.;<br>- major functional upgrades at a minimum once per year in agreement with the Authority; |

| | |
|---|---|
| | - incremental upgrades as needed for fault resolution of incidents of Priority 3 and above. |
| C.5.8 | The Supplier shall inform the Authority about incidents within 1 hour of occurrence (as defined by active monitoring or incident) with notifications delivered via email to the nominated DE&S point(s) of contact or mailbox(es). Points of Contact will be nominated by the Authority during the Implementation phase. |
| C.5.9 | The Supplier shall inform the Authority about security incidents within 20 minutes of occurrence (as defined by active monitoring or incident) with notifications delivered via email to the nominated DE&S point(s) of contact or mailbox(es). Points of Contact will be nominated by the Authority during the implementation of DES AIMS. |
| **C.6 - Contract Management and Reporting** | |
| C.6.1 | The Supplier shall attend monthly contract management meetings to be held remotely via a virtual meeting group |
| C.6.2 | The Supplier shall provide monthly service performance reports within 10 working days of the end of the month to include comprehensive data about the services provided under Part C – DES AIMS service to reflect the SLA and DES AIMS system administration SLA. |
| **C.7 - Exit Strategy** | |
| C.7.1 | The Supplier shall deliver to the Authority, during the implementation period, an Exit Plan detailing the approach the supplier will take to ensure the smooth transition to any successor system and return the data held within the AIM Software. |
| C.7.2 | The supplier shall provide the Authority sufficient assistance and information as necessary to enable an efficient and effective transfer of airworthiness data to any successor. |
| C.7.3 | Data shall be presented to the Authority as and when required in a format that is capable of being fully utilised by the authority within 5 working days of being requested. |
| C.7.4 | There shall be no adverse impact to the Authority's ability to maintain airworthiness management during the execution of the exit plan. |
| C.7.5 | The Supplier will continue to provide airworthiness management software during the exit process without disruption or deterioration of the authority's requirements detailed in this document. |
| C.7.6 | All parties shall review, update, and agree the exit plan every six months starting at the commencement of the Contract. Additional reviews may also take place at a time where either the Authority or the Contractor deem necessary to ensure it remains relevant to the authority's development solutions and reflects any change in services. The review is to consider changing technologies and amendments brought on through changes made to the scope or nature of DES AIMS. The review output must include updates to the supporting technical documentation describing the detailed information held within the AIMS Exit DB. |
| **C.8 – New User and top-up training** | |
| C.8.1 | The Supplier's responsibilities shall include provision of training for up to 1200 Authorised Users per annum, detailed in the Training Plan. This shall be conducted using appropriate training methods and approaches to enable Authorised Users to operate the DES AIMS competently. |
| C.8.2 | The Supplier shall provide top-up training to all Authorised Users, where changes are made to the DES AIMS software, detailed in the Training Plan using appropriate training methods and approaches for any new features and / or services being provided on the DES AIMS. |
| **C.9 - Additional Services** | |
| C.9.1 | The Supplier shall provide additional DE&S Airworthiness Issue Management Services in accordance with an Additional Tasking Process. The scope of that work includes:<br>- Interface and data uploading services;<br>- Configuration services;<br>- Training services including face-to-face and tailored training materials, |

| | |
|---|---|
| | - Data migration services;<br>- Data archiving services;<br>- Technical subject matter expertise;<br>- MoD Data processing activities (this shall include the need for Supplier employees shall sign a DEFFORM 702 (Employee's Acknowledgement to Employer of Obligations Relating to Confidentiality) where any MoD data will need to be processed) |

**Part D –DES AIMS supporting requirements**

| Serial | Requirement |
|---|---|
| 1 | All Supplier personnel working on the DES AIMS shall be UK based and SC cleared (or if working towards this must have basic level clearance (BPSS)). Clearance details must be provided to the Authority for review and confirmation prior to the commencement of the service. |
| 2 | The solutions devised to the DES AIM requirements shall be compatible with the requirements set out in JSP 248[1] governing the handling of United States of America Export Controlled Data (ECD): in essence the Supplier will demonstrate adequate controls in its software and services (e.g. administrative support) to protect against unauthorized access, disclosure and transfer of ECD. |
| 3 | The Supplier shall engage with Delivery Teams during the Implementation phase to determine whether information to be held on the DES AIMS solution is ECD and, if so, provide such information as the DT may require for purposes of demonstrating compliance with JSP 248. |

[1] Of especial relevance is Part 2, sections 2 (in particular "Authorisation of access to ECD for the MOD or third-party contractors") and 3 (Managing ECD).

# Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract.

During the Term the Buyer may offboard Platform / Delivery Teams as required by providing the Supplier with two weeks' notice. The Call-Off Contract Charges detailed in the tables below are the Total Maximum Price. The Supplier will only charge the Buyer for Platforms / Delivery Teams which have not been offboarded and are using the DE&S Airworthiness Issues Management System (RESOLVE) tool on a monthly basis.

The detailed Charges breakdown for the provision of Services during the Term will include:

**Table 1 – Year 1 (01 April 2023 – 31 March 2024)**

[REDACTED]

**Table 2 –Year 2 (01 April 2024 – 31 March 2025)**

[REDACTED]

**Table 3 – Option Year 1 (01 April 2025 – 31 March 2026)**

[REDACTED]

**Table 4 – Option Year 2 (01 April 2026 – 31 March 2027)**

[REDACTED]

**Table 5 – User Base Description**

| User Base | Description |
|---|---|
| Small | 1-99 users |
| Medium | 100-299 users |
| Large | 300-599 users |
| Extra Large | 600 or more users |

**Table 6 - Monthly Subscription Charges**

| Monthly Subscription | | | | | | |
|---|---|---|---|---|---|---|
| | **Issue Management** | **Read Only (Archive)** | **Electronic Library** | **Quality Management** | **Data Integration (External)** | **Business Analytics Level 1** |
| Service | £7,000.00 | £3,000.00 | £4,000.00 | £3,000.00 | £5,000.00 | £2,000.00 |
| | | | | | | |

| **Number of Business Process Models** | | | | | | |
|---|---|---|---|---|---|---|
| Less than 4 | - | - | N/A | N/A | N/A | N/A |
| 4-10 | £4,000.00 | - | N/A | N/A | N/A | N/A |
| 11-20 | £7,000.00 | - | N/A | N/A | N/A | N/A |
| More than 20 | £10,000.00 | - | N/A | N/A | N/A | N/A |
| **User Base** | | | | | | |
| Small | - | - | - | - | - | - |
| Medium | £3,000.00 | - | £800.00 | £500.00 | - | £1,000.00 |
| Large | £6,000.00 | - | £1,200.00 | £1,000.00 | - | £1,500.00 |
| Extra Large | £10,000.00 | - | £1,500.00 | £2,000.00 | - | £2,000.00 |

## Customer Benefits

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

G-Cloud 12 Customer Benefits Record

# Part B: Terms and conditions

## 1. Call-Off Contract Start date and length

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

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

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

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

## 2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection

- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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' 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 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

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

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

## 3. Supply of services

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

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

## 4. Supplier staff

4.1 The Supplier Staff must:

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 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

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

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

## 5. Due diligence

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

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 its own due diligence

## 6. Business continuity and disaster recovery

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

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

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

## 7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

7.11 If there's an invoice dispute, the Buyer must pay the undisputed 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 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

## 11. Intellectual Property Rights

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

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

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

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

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

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

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

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

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

11.6.2 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

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

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

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

11.7.3 other material provided by the Buyer necessary for the Services

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

## 12. Protection of information

12.1 The Supplier must:

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

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

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

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

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

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

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

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

## 13. Buyer data

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

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

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

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

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

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

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

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-management-approach 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/technology-code-of-practice/technology-code-of-practice

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

13.6.6 buyer requirements in respect of AI ethical standards.

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

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

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

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

## 14. Standards and quality

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

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/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 (and the Buyer of any Buyer Confidential Information breach). 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 is reasonable compensation and covers all the Supplier's avoidable costs or Losses

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

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

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); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)

- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (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 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.

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

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

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

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

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 the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

## 24. Liability

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

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

## 25. Premises

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

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

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

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

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

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

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

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

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

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

29.6.1 its failure to comply with the provisions of this clause

29.6.2 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

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

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

## 30. Additional G-Cloud services

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

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

## 31. Collaboration

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

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

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

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

## 32. Variation process

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

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

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

## 33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

# Schedule 3: Collaboration agreement

Not Applicable.

# Schedule 4: Alternative clauses

.

Not Applicable.

# Schedule 5: Guarantee

Not Applicable.

# Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

| **Expression** | Meaning |
|---|---|
| **Action** | An activity (including authorisations against decisions) assigned to a User as part of the execution of a Process whilst responding to an Event or managing an Issue. |
| **Additional Services** | Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request. |
| **Admission Agreement** | The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s). |
| **Air Safety** | The state of freedom from unacceptable risk of injury to persons, or damage, throughout the life cycle of military Air Systems. Its purview extends across all Defence Lines of Development and includes Airworthiness, Flight Safety, policy, regulation and the apportionment of resources. It does not address survivability in a hostile environment. |
| **Air System** | A fixed or rotary wing aircraft, piloted or remotely piloted, and the ground-based systems vital to their safe operation. |
| **Air System Document Set (ADS)** | means the documentation considered as essential for sustaining the Type Airworthiness and maintaining the continuing Airworthiness, and for ensuring the safe operation of an Air System. The documentation is defined, maintained and approved for use by the Type Airworthiness Authority. |
| **Airworthiness** | The ability of an Air System or other airborne equipment or system to be operated in flight and on the ground without significant hazard to aircrew, ground crew, passengers or to third parties; it is a technical attribute of materiel throughout its lifecycle. |
| **Airworthiness Issues** | Equipment faults/failings that may impact airworthiness, air-safety, availability and/or operating capability of air systems/equipment. Airworthiness Issues can be reported from a range of sources: Front Line Commands; Design |

| | |
|---|---|
| | Organisations; DE&S; and other operating nations (through a DE&S interface). They are often interdependent, linked or could be merged into one another. Appropriate actions to investigate and respond to many of them are strictly governed by Military Aviation Authority (MAA) Regulations. |
| **Application** | The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace). |
| **Artefacts** | Discrete data items (i.e an airworthiness related document that can be used as evidence in making an airworthiness judgement) attached to an Issue or Entity to form part of the evidence trail. |
| **Audit** | An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any). |
| **Authorised User(s)** | Any person having been given access to the DES AIMS by the Authority. This will include, but is not limited to, people within DE&S, Front Line Commands, Design Organisations and industry partners. |
| **Authority to Operate (AtO)** | means the risks or issues introduced by the service are accepted and the service has proven it can meet the Users needs. The service is authorised to operate within its agreed parameters. Only when the service deviates beyond these parameters will it be required to revisit the release process. An AtO is given to projects following a successful probationary period after the introduction or change to an ICT Service. It is issued by the Network Operating Authority following its assessment of behavior of the Service. |
| **Authority to Test (AtT)** | means the authority to release the service tied to the scope requested within the technical release readiness assessment and associated test plans. At this stage authority will be granted if the risks are deemed acceptable against the scope of testing, there maybe risks that are not necessarily acceptable for IAtO. |
| **Authority Zone** | Authority Zones focus on the level of security governance and document control officer coverage that the MoD is able to exercise over services. This reflects the freedom of action |

| | |
|---|---|
| | which the MoD has over such services and the ability the MoD has to directly respond to threats to the MoD's ICT based information assets. |
| **Background IPRs** | For each Party, IPRs:<br>• 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<br>• created by the Party independently of this Call-Off Contract, or<br><br>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software. |
| **Buyer** | The contracting authority ordering services as set out in the Order Form. |
| **Buyer Data** | All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer. |
| **Buyer Personal Data** | The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract. |
| **Buyer Representative** | The representative appointed by the Buyer under this Call-Off Contract. |
| **Buyer Software** | Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services. |
| **Call-Off Contract** | This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement. |
| **Charges** | The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract. |

| | |
|---|---|
| **Collaboration Agreement** | An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate. |
| **Commercially Sensitive Information** | Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive. |
| **Confidential Information** | Data, Personal Data and any information, which may include (but isn't limited to) any:<br>• 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<br>• 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<br><br>Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly. |
| **Controller** | Takes the meaning given in the GDPR. |
| **Critical Acceptance Criteria** | Pre-established standards or requirements a product or project must meet. |
| **Crown** | The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf. |
| **DART** | The Defence Assurance Risk tool which is used to enable anyone with an account to initiate, input to and track various information assurance related requirements |

| | |
|---|---|
| **Data Loss Event** | Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach. |
| **Data Protection Impact Assessment (DPIA)** | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data. |
| **Data Protection Legislation (DPL)** | Data Protection Legislation means:<br>(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time<br>(ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy<br>(iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner |
| **Data Subject** | Takes the meaning given in the GDPR |
| **DE&S Airworthiness Management System (DES AIMS)** | The off-the shelf software package being procured by DE&S to meet their software requirement for an off the shelf Airworthiness Issues Management System in accordance with the requirement Part A of Schedule 1 above that enables all Airworthiness Issues to be identified, reported and managed. Management of Airworthiness Issues is the undertaking of processes, tasks and actions to resolve them, and the ability to monitor progress of the Airworthiness Issue. |
| **Default** | Default is any:<br>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)<br>• 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<br><br>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer. |

| | |
|---|---|
| **Deliverable(s)** | The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract. |
| **Design Organisation** | Means the approved organisation responsible for the overall design or through-life configuration management of the design of each product, part or appliance installed in an Air System. |
| **DGAPI** | DG (Director General) Air Policy Instructions are DE&S internal policies used to govern activities within the air environment. |
| **DH's Area of Responsibility (AoR)** | Means the Air Systems (and related teams, personnel and processes) a Duty Holder is responsible for. |
| **Digital Marketplace** | The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/) |
| **DNS** | The Domain Name System is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. |
| **DPA 2018** | Data Protection Act 2018. |
| **Duty Holder (DH)** | means the individual legally accountable for the safe operation of Air Systems in their AoR and for ensuring that risks to life are as low as reasonably practicable and tolerable. DH have a personal level duty of care for the personnel under their command; those who, by virtue of their temporary involvement in aviation activities, come within an DH's Area of Responsibility (AoR); and the wider public who may be affected by their operations. |
| **Employment Regulations** | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive. |
| **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-for-tax |
| **End** | Means to terminate; and Ended and Ending are construed accordingly. |
| **Entity(ies)** | The artefacts and data produced as an outcome of executing Processes end to end. Creating a record of all Actions and decisions made throughout a Process to assist in the management of an Issue or Event. |
| **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. |
| **Event** | Any unforeseen in-service arising relating to an Air System that someone believes might compromise airworthiness and therefore requires the attention of the Type Airworthiness Authority. These events come from a number of sources in multiple formats. Events may be escalated to an Issue or linked to existing issues. |
| **Expiry Date** | The expiry date of this Call-Off Contract in the Order Form. |
| **Export** | The ability to create a data file that can be utilised outside of the DES AIMS to provide input (in accordance with defined data dictionary entries) into another key air environment tools (either MoD or Industry owned), provide an output of data in support of other MoD processes (air investigations for example), provide output in support of DE&S corporate |

| | |
|---|---|
| | dashboards or to provide full output of the AIMS for the purposes of transition to another future AIMS tool. |
| **Flight Safety** | means a collective endeavour to operate in the air environment safely, it embraces any activity that contributes to the safe operation of military airworthy systems in flight or on the ground. |
| **Force Majeure** | A force Majeure event means anything affecting either Party's performance of their obligations arising from any:<br>• acts, events or omissions beyond the reasonable control of the affected Party<br>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare<br>• acts of government, local government or Regulatory Bodies<br>• fire, flood or disaster and any failure or shortage of power or fuel<br>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available<br><br>The following do not constitute a Force Majeure event:<br>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain<br>• 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<br>• the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into<br>• any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans |
| **Former Supplier** | A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor). |
| **Framework Agreement** | The clauses of framework agreement RM1557.12 together with the Framework Schedules. |
| **Fraud** | Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this |

| | |
|---|---|
| | Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown. |
| **Freedom of Information Act or FoIA** | The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation. |
| **Front Line Command (FLC)** | The single-Service Commands (Navy, Land or Air) responsible for operating, administering or training its forces outside the requirements of joint operations. |
| **G-Cloud Services** | The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement. |
| **GDPR** | General Data Protection Regulation (Regulation (EU) 2016/679) |
| **Good Industry Practice** | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances. |
| **Government Procurement Card** | The government's preferred method of purchasing and payment for low value goods or services. |
| **Guarantee** | The guarantee described in Schedule 5. |
| **Guidance** | Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence. |

| | |
|---|---|
| **Implementation Plan** | The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding. |
| **Indicative test** | ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6. |
| **Information** | Has the meaning given under section 84 of the Freedom of Information Act 2000. |
| **Information security management system** | The information security management system and process developed by the Supplier in accordance with clause 16.1. |
| **Inside IR35** | Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool. |
| **Insolvency event** | Can be:<br>• a voluntary arrangement<br>• a winding-up petition<br>• the appointment of a receiver or administrator<br>• an unresolved statutory demand<br>• a Schedule A1 moratorium |
| **Intellectual Property Rights or IPR** | Intellectual Property Rights are:<br>• 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<br>• 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<br>• all other rights having equivalent or similar effect in any country or jurisdiction |
| **Interim Authority to Operate (IAtO)** | Means the approval given by the Authority where the risks or issues introduced by the service are known and deemed to be acceptable to allow the system to connect to the network for a probationary period of up to 6 months, to test and verify in the live environment, prior to full AtO being granted. |

| | |
|---|---|
| **Intermediary** | For the purposes of the IR35 rules an intermediary can be:<br>• the supplier's own limited company<br>• a service or a personal service company<br>• a partnership<br><br>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency). |
| **IPR claim** | As set out in clause 11.5. |
| **IR35** | IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary. |
| **IR35 assessment** | Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35. |
| **Issue** | A means for capturing, escalating, investigating and resolving events (singular or multiple linked together) that could compromise the airworthiness of the Air System. An Issue allows an easily accessible audit trail of activities, actions and decisions aimed at mitigating risk to an Air System. |
| **Know-How** | All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date. |
| **Law** | Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply. |
| **LED** | Law Enforcement Directive (EU) 2016/680. |

| | |
|---|---|
| **Loss** | All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly. |
| **Lot** | Any of the 3 Lots specified in the ITT and Lots will be construed accordingly. |
| **Malicious Software** | Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence. |
| **Management Charge** | The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract. |
| **Management Information** | The management information specified in Framework Agreement section 6 (What you report to CCS). |
| **Material Breach** | Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract. |
| **Military Aviation Authority (MAA)** | The Military Aviation Authority is an independent organisation responsible for regulating Air Safety across defence. MAA is part of the Ministry of Defence. |
| **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. |
| **MODNet** | The Ministry of Defence Office 365-based internal communications and collaboration system. |

| | |
|---|---|
| **MRP** | MAA Regulatory Publications |
| **New Fair Deal** | The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended. |
| **Order** | An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes. |
| **Order Form** | The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services. |
| **Ordered G-Cloud Services** | G-Cloud Services which are the subject of an order by the Buyer. |
| **Outside IR35** | Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool. |
| **Party** | The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly. |
| **Personal Data** | Takes the meaning given in the GDPR. |
| **Personal Data Breach** | Takes the meaning given in the GDPR. |
| **Platform** | Means DE&S Delivery Teams. |
| **Process(es)** | The execution of various workflows with associated tasks or Actions with the aim of providing a resolution to any event or issue (processes and workflows are defined in Appendix 3. |
| **Processing** | Takes the meaning given in the GDPR. |
| **Processor** | Takes the meaning given in the GDPR. |

| | |
|---|---|
| **Prohibited act** | To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:<br>• induce that person to perform improperly a relevant function or activity<br>• reward that person for improper performance of a relevant function or activity<br>• commit any offence:<br>  ○ under the Bribery Act 2010<br>  ○ under legislation creating offences concerning Fraud<br>  ○ at common Law concerning Fraud<br>  ○ committing or attempting or conspiring to commit Fraud |
| **Project Specific IPRs** | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs. |
| **Property** | Assets and property including technical infrastructure, IPRs and equipment. |
| **Protective Measures** | Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it. |
| **PSN or Public Services Network** | The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources. |
| **Recovery Point Objective (RPO)** | means the maximum targeted period in which data might be lost from an IT service due to a major incident. |
| **Recovery Time Objective (RTO)** | means the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. |

| | |
|---|---|
| **Regulatory body or bodies** | Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract. |
| **Relevant person** | Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body. |
| **Relevant Transfer** | A transfer of employment to which the employment regulations applies. |
| **Replacement Services** | Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party. |
| **Replacement supplier** | Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer). |
| **RMADS** | The Risk Management and Accreditation Document Set that sets out the system, the identified risks, the security controls applied and lists all the applicable documents to accreditation, risk and other through life management activities. This is reviewed by the accreditor and subsequently approved. |
| **Security management plan** | The Supplier's security management plan developed by the Supplier in accordance with clause 16.1. |
| **Service data** | Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data. |
| **Service definition(s)** | The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement. |
| **Service description** | The description of the Supplier service offering as published on the Digital Marketplace. |

| | |
|---|---|
| **Service Level Agreement (SLA)** | A contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. |
| **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. |
| **Services** | The services ordered by the Buyer as set out in the Order Form. |
| **Spend controls** | The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service |
| **Start date** | The Start date of this Call-Off Contract as set out in the Order Form. |
| **Subcontract** | Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof. |
| **Subcontractor** | Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services. |
| **Subprocessor** | Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract. |
| **Supplier** | The person, firm or company identified in the Order Form. |
| **Supplier Representative** | The representative appointed by the Supplier from time to time in relation to the Call-Off Contract. |
| **Supplier staff** | All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors |

| | |
|---|---|
| | used in the performance of its obligations under this Call-Off Contract. |
| **Supplier terms** | The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application. |
| **Term** | The term of this Call-Off Contract as set out in the Order Form. |
| **Type Airworthiness Authority (TAA)** | The individual who on behalf of the Secretary of State, oversees the airworthiness of specified Air System types. |
| **User** | Authorised User. |
| **Variation** | This has the meaning given to it in clause 32 (Variation process). |
| **Working Days** | Any day other than a Saturday, Sunday or public holiday in England and Wales. |
| **Year** | A contract year. |

# Schedule 7: GDPR Information

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

## Annex 1: Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are: DES-DPO-Mailbox@mod.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are: Anthony Harris, Commercial Director tharris@tlmnexus.com

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

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

| Descriptions | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**<br><br>The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:<br><br>● The Personal Data controlled by the Buyer and processed by the Supplier will be in order for the Supplier to create, maintain and manage user accounts. The Supplier will hold Personal Data including Names, Email Addresses and Telephone Numbers. |
| Duration of the Processing | In accordance with this Call-off Contract Start date and Expiry date. |
| Nature and purposes of the Processing | The Personal Data controlled by the Buyer and processed by the Supplier will be in order for the Supplier to create, maintain and manage user accounts. The Supplier will hold Personal Data including Names, Email Addresses and Telephone Numbers. |
| Type of Personal Data | Name, address, telephone number. |

| | |
|---|---|
| Categories of Data Subject | Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers. |
| Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data | The Personal Data will be retained for the term of this Call-off Contract and will be destroyed on expiry. |

# Appendix 1 – Service Levels, Service Level Agreements and Service Credits

[REDACTED]

# Appendix 2 - Implementation Plan

[REDACTED]

# Appendix 3 – Exit Strategy

[REDACTED]

# Appendix 4 – Training Plan

[REDACTED]

# Appendix 5 – User Access Control

[REDACTED]

# Appendix 6 – Business Continuity and Disaster Recovery

[REDACTED]

# Appendix 7 – Additional Tasking Process

1. BACKGROUND

1.1. The Supplier shall not commence the carrying out of any Additional Services without obtaining the prior consent of the Authority in accordance with this Schedule. If the Supplier fails to obtain such consent the Supplier shall have no recourse against the Authority in respect of any costs or liabilities incurred.

2. TASK ORDER

2.1. The Authority may request Additional Services by issuing an additional task order form to the Supplier as set out in Annex A to this Appendix. The Supplier shall within five (5) business days of receipt of the additional task order form, complete Parts 2 and 3 of Annex A to this Schedule and return it to the Authority.

2.2. The Authority shall as soon as reasonably practicable do one of the following:

2.2.1. authorise the additional task order form by completing Part 3 of the relevant additional task order form and returning the form to the Supplier;

2.2.2. in its absolute discretion reject the additional task, in which case it shall notify the Supplier of the rejection; or

2.2.3. require the Supplier to modify Parts 2 and / or 3 of the additional task order form in which case the Supplier shall make such modifications and provide the Authority with an updated additional task order form within such period specified by the Authority or if no period is specified, within five (5) Business Days of such request (in which case the Authority shall have the rights set out in this paragraph 2 in relation to the updated additional task order form.

2.3. The Payment of the additional services received shall be made to the Supplier in accordance with the Part 2 of the additional task order form.

3. COSTS

3.1. Unless expressly agreed otherwise by the Authority in writing in relation to a particular additional service, the Supplier shall be responsible for its own costs and expenses incurred in the preparation and assessment of any additional task order form.

## Annex A to Appendix 7 – Tasking Order Form to 703454451 (DCT002).

To:

**Part 1: Requirement**

| | |
|---|---|
| **TASK ID**:<br><br>**DATE RAISED:**<br><br>**PO Number:** | **TASK NAME:**<br><br>**DELIVERY TIME:** |

**Statement of Work including Deliverables, Acceptance Criteria, and special conditions for delivery:**

**DESCRIPTION:**

**ASSUMPTION & DEPENDENCIES**

- 

**EXPECTED DELIVERABLE OUTPUT (outline):**

| SERIAL | OUTPUT DESCRIPTION | Deliverable | Delivery schedule | ACCEPTANCE CRITERIA |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |

Note: Confirmation that the Serials have been delivered and the acceptance criteria has been met must be provided to the Buyer commercial point of contact for this Tasking Order Form and prior to requesting for payment to be processed.

**Important Notes for Supplier:**

- 

**Part 2: Supplier Proposal**

**OVERVIEW OF SUPPLIER DELIVERY**

**PAYMENT PLAN:**

The maximum price achievable for each Serial shall be subject to achievement of the Acceptance Criteria. All payments are payable in arrears and subject to achieving the Acceptance Criteria.

| Milestone | Description | Delivery Date | % | Acceptance Criteria | Maximum price £ (excl. VAT) subject to meeting the Critical Acceptance Criteria |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| | | | | **Total Maximum Price (ex VAT)** | £ |

(*Maximum Cost – Part 1 above)

The above payment plan is based on the Supplier's assessment of the following recourses required to deliver the outputs:

| SFIA Level | Day Rate | Days | TOTAL MAXIMUM PRICE (ex VAT) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | **TOTAL MAXIMUM PRICE (Ex. VAT)** | £ |

**Travel & Subsistence (T&S)**

| Description | Maximum £ (incl. VAT) |
|---|---|
| Expenses T&S (maximum) supported by receipts, travel expenses allowable from usual place of residence to MoD, Bristol Abbey Wood or other work site as approved by MoD DE&S. The maximum Travel & Subsistence is payable in line with MOD Policy. | £ |

**Part 3. Buyer Authorisation**

Note: The Supplier shall not proceed with the Tasking Order Form until a fully authorised Tasking Order Form has been received

| | | |
|---|---|---|
| **BUYER REPRESENATIVE AUTHORISATION** | **NAME:** | |
| | **SIGNATURE:** | |
| | **TITLE:** | |
| | **DATE:** | |

| | | |
|---|---|---|
| **BUYER COMMERCIAL AUTHORISATION** | **NAME:** | |
| | **SIGNATURE:** | |
| | **TITLE:** | |
| | **DATE:** | |

| | | |
|---|---|---|
| **SUPPLIER ACCEPTANCE** | **NAME:** | |
| | **SIGNATURE:** | |
| | **TITLE:** | |
| | **DATE:** | |

## Annex B Appendix 7 – Rate Card for Additional Services

**Day Rate in UK £ against each level and activity**

| | Strategy and architecture | Business change | Solution development and implementation | Service management | Procurement and management support | Client interface |
|---|---|---|---|---|---|---|
| **1. Follow** | N/A | N/A | N/A | N/A | N/A | N/A |
| **2. Assist** | 527 | 527 | 527 | 527 | 527 | 527 |
| **3. Apply** | 659 | 659 | 659 | 659 | 659 | 659 |
| **4. Enable** | 854 | 854 | 854 | 854 | 854 | 854 |
| **5. Ensure or advise** | 1036 | 1036 | 1036 | 1036 | 1036 | 1036 |
| **6. Initiate or influence** | 1318 | 1318 | 1318 | 1318 | 1318 | 1318 |
| **7. Set strategy or inspire** | 1469 | 1469 | 1469 | 1469 | 1469 | 1469 |

## Annex C to Appendix 7 – Additional Skill Levels Defined

| Level | Autonomy | Influence | Complexity | Business Skills |
|---|---|---|---|---|
| 1 Follow | Works under close supervision. Uses little discretion. Is expected to seek guidance in expected situations. | Interacts with immediate colleagues. | Performs routine activities in a structured environment. Requires assistance in resolving unexpected problems. | Uses basic information systems and technology functions, applications, and processes. Demonstrates an organised approach to work. Learns new skills and applies newly acquired knowledge. Has basic oral and written communication skills. Contributes to identifying own development opportunities. |
| 2 Assist | Works under routine supervision. Uses minor discretion in resolving problems or enquiries. Works without frequent reference to others. | Interacts with and may influence immediate colleagues. May have some external contact with Authority's and Contractors. May have more influence in own domain. | Performs a range of varied work activities in a variety of structured environments. | Understands and uses appropriate methods, tools and applications. Demonstrates a rational and organised approach to work. Is aware of health and safety issues. Identifies and negotiates own development opportunities. Has sufficient communication skills for effective dialogue with colleagues. Is able to work in a team. Is able to plan, schedule and monitor own work within short time horizons. Absorbs technical information when it is presented systematically and applies it effectively. |
| 3 Apply | Works under general supervision. Uses discretion in identifying and resolving complex problems and assignments. Usually receives specific instructions and has work reviewed at frequent milestones. Determines when issues should be escalated to a higher level. | Interacts with and influences department/project team members. May have working level contact with Authority's and Contractors. In predictable and structured areas may supervise others. Makes decisions which may impact on the work assigned to individuals or phases of projects. | Performs a broad range of work, sometimes complex and non-routine, in a variety of environments. | Understands and uses appropriate methods, tools and applications. Demonstrates an analytical and systematic approach to problem solving. Takes the initiative in identifying and negotiating appropriate development opportunities. Demonstrates effective communication skills. Contributes fully to the work of teams. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation and procedures. Absorbs and applies technical information. Works to required standards. Understands and uses appropriate methods, tools and applications. Appreciates the wider field of information systems, and how own role relates to other roles and to the business of the employer or client. |
| 4 Enable | Works under general direction within a clear framework of accountability. | Influences team and specialist peers internally. Influences Authority's at account level and Contractors. Has some | Performs a broad range of complex technical or professional work activities, in a variety of contexts. | Selects appropriately from applicable standards, methods, tools and applications. Demonstrates an analytical and systematic approach to problem solving. Communicates fluently orally and in writing, |

| | | | | |
|---|---|---|---|---|
| | Exercises substantial personal responsibility and autonomy. Plans own work to meet given objectives and processes. | responsibility for the work of others and for the allocation of resources. Participates in external activities related to own specialism. Makes decisions which influence the success of projects and team objectives. | | and can present complex technical information to both technical and non-technical audiences. Facilitates collaboration between stakeholders who share common objectives. Plans, schedules and monitors work to meet time and quality targets and in accordance with relevant legislation and procedures. Rapidly absorbs new technical information and applies it effectively. Has a good appreciation of the wider field of information systems, their use in relevant employment areas and how they relate to the business activities of the employer or client. Maintains an awareness of developing technologies and their application and takes some responsibility for personal development. |
| 5 Ensure /Advise | Works under broad direction. Is fully accountable for own technical work and/or project/ supervisory responsibilities. Receives assignments in the form of objectives. Establishes own milestones and team objectives, and delegates responsibilities. Work is often self-initiated. | Influences organisation, customers, contractors and peers within industry on the contribution of own specialism. Has significant responsibility for the work of others and for the allocation of resources. Makes decisions which impact on the success of assigned projects i.e. results, deadlines and budget. Develops business relationships with the Authority. | Performs a challenging range and variety of complex technical or professional work activities. Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer/ organisational requirements. | Advises on the available standards, methods, tools and applications relevant to own specialism and can make correct choices from alternatives. Analyses, diagnoses, designs, plans, execute and evaluates work to time, cost and quality targets. Communicates effectively, formally and informally, with colleagues, subordinates and customers. Demonstrates leadership. Facilitates collaboration between stakeholders who have diverse objectives. Understands the relevance of own area of responsibility/ specialism to the employing organisation. Takes customer requirements into account when making proposals. Takes initiative to keep skills up to date. Mentors more junior colleagues. Maintains an awareness of developments in the industry. Analyses requirements and advises on scope and options for operational improvement. Demonstrates creativity and innovation in applying solutions for the benefit of the Authority. |
| 6 Initiate/ Influence | Has defined authority and responsibility for a significant area of work, including technical, financial and quality aspects. Establishes organisational objectives and delegates responsibilities. Is accountable for actions and | Influences policy formation on the contribution of own specialism to business objectives. Influences a significant part of own organisation and influences the Authority/contractors and industry at senior management | Performs highly complex work activities covering technical, financial and quality aspects. Contributes to the formulation of IT strategy. Creatively applies a wide range of technical | Absorbs complex technical information and communicates effectively at all levels to both technical and non-technical audiences. Assesses and evaluates risk. Understands the implications of new technologies. Demonstrates clear leadership and the ability to influence and persuade. Has a broad understanding of all aspects of IT and deep understanding of own specialism(s). Understands |

| | | | | |
|---|---|---|---|---|
| | decisions taken by self and subordinates. | level. Makes decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance. Develops high-level relationships with the Authority, contractors and industry leaders. | and/or management principles. | and communicates the role and impact of IT in the employing organisation and promotes compliance with relevant legislation. Takes the initiative to keep both own and subordinates' skills up to date and to maintain an awareness of developments in the IT industry. |
| 7 Set Strategy/ Inspire | Has authority and responsibility for all aspects of a significant area of work, including policy formation and application. Is fully accountable for actions taken and decisions made, both by self and subordinates | Makes decisions critical to organisational success. Influences developments within the IT industry at the highest levels. Advances the knowledge and/or exploitation of IT within one or more organisations. Develops long-term strategic relationships with customers and industry leaders. | Leads on the formulation and application of strategy. Applies the highest level of management and leadership skills. Has a deep understanding of the IT industry and the implications of emerging technologies for the wider business environment | Has a full range of strategic management and leadership skills. Understands, explains and presents complex technical ideas to both technical and non-technical audiences at all levels up to the highest in a persuasive and convincing manner. Has a broad and deep IT knowledge coupled with equivalent knowledge of the activities of those businesses and other organisations that use and exploit IT. Communicates the potential impact of emerging technologies on organisations and individuals and analyses the risks of using or not using such technologies. Assesses the impact of legislation, and actively promotes compliance. Takes the initiative to keep both own and subordinates' skills up to date and to maintain an awareness of developments in IT in own area(s) of expertise. |

# Appendix 8 – Security Aspect Letter

[REDACTED]