

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

### Order Form

This Order Form is for the provision of the Call-Off Deliverables. It is issued under the DIPS Framework Contract with a unique reference number starting with RM6249. The DIPS Framework and this Call-Off Contract are to be for the delivery of Outcomes only. This Framework is not for the request and delivery of resource. If specific resources are needed alternative sourcing methods must be used.

During the Call-Off Contract Period, the Requirement Holder and the Supplier may agree and execute a Statement of Work (in the form of the template set out in Appendix 4 to this Framework Schedule 6 (Order Form Template, Statement of Requirements Template)). Upon execution of any Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

The Parties agree that when the Requirement Holder seeks further Deliverables within the initial scope of the original Call-off contract from the Supplier that are not provided for in this Call-Off Contract, the Requirement Holder and Supplier will agree and execute a Call-Off Variation Form.

All capitalised terms in this Order Form shall have the meanings set out in Joint Schedule 1 (Definitions) unless otherwise stated.

### 1a. Identification

Call-Off Lot	Lot 1 - Solution, Enterprise and Technical Architecture, Data, Inovation, Technical Assurance and Knowledge & Information Management				
Call-Off Reference	RM6249/DIPS(1)034	Version Number	V2.0	Date	19/08/2024
Business Case Reference	Original FBC Number	BMfS Data Catalogue & Reference Data Manager Content Creation V1.0			
	Amendment FBC Number				
Project / equipment for which Services are in support	Business Modernisation for Support Data Catalogue	Urgent Capability Requirement (UCR)		N/A	
Call-Off Contract title:	BMfS Data Catalogue & Reference Data Manager Content Creation				
Call-Off Contract description:	The high-level objective of this activity is for the supplier to source and load DefSp metadata content into the Data Catalogue service, design and configure the Informatica R360 Reference Data Management service, source and load Reference Data records into the Reference Data Management service and implement Reference Data Management procedures. A full overview of the objectives, deliverables and intent is within the Statement of Requirement.				

### 1b. Contact details

Government Directorate / Organisation Title	Defence Support Major Programmes (Def Sp MP)	Name of Supplier	KPMG LLP
Name of Requirement		Name of Supplier's	

**DIPS Order Form / Statement of Requirements Template  
(Framework Schedule 6)**

Holder's Authorised Representative		Authorised Representative	
Post title	ODS & DSI Delivery Lead	Post title	Director
Requirement Holder's Address	NH3, Cedar 2A, MOD Abbeywood Bristol	Supplier Address	15 Canada Square, London

Postcode	BS34 8JH	Postcode	E14 5GL
Telephone		Telephone	
Email		Email	
Unit Identification Number (UIN)		Value Added Tax (VAT) Code	
Resource Accounting Code (RAC)	NNB004		
Name of Requirement Holder's Project Lead			
Requirement Holder's Secondary Contact Name		Supplier Secondary Contact Name	
Requirement Holder's Secondary Contact Role	BMfS Programme Delivery Manager - Enablers	Supplier Secondary Contact Role	Senior Account Manager
Requirement Holder's Secondary Contact Email		Supplier Secondary Contact Email	
Date that the Statement of Requirements was issued		Deadline for Requirement Holder's receipt of Supplier's Call-Off Tender	
19/08/2024		02/10/2024	

**1c. Statement of Requirements (SOR) (This section 1c. to be completed in full OR a complete SOR to be attached in Appendix 7 of this document)**

Unique Order Number (defined by delivery team)	N/A	
SOR version issue number	V2.0	SOR dated 19/08/2024
SOR title	BMfS Data Catalogue & Reference Data Manager Content Creation	

Background/justification for Call-Off Contract
Please see SOR attached in Appendix 6
Description of Services to be provided under the Call-Off Contract
Please see SOR attached in Appendix 6

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Activities required to be undertaken under the Call-Off Contract
Please see SOR attached in Appendix 6
Outputs to be provided under the Call-Off Contract
Please see SOR attached in Appendix 6
Acceptance/rejection criteria / provisions
Please see SOR attached in Appendix 6
Material KPIs / Critical Service Level Failure
N/A

SOR approved by (Name in capital letters)		Telephone	
Directorate / Division	UK StratCom	Email	

## Material KPIs

N/A

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The following shall constitute a Critical Service Level Failure for the purposes of this Call-Off Contract in accordance with Call-Off Schedule 14 (Service Levels):

## Critical Service Level Failure

N/A

The applicable Service Levels are as specified in Annex A to Part A of Call-Off Schedule 14 (Service Levels).

List all Requirement Holder Assets applicable to the Services that shall be issued to the Supplier and returned to the Requirement Holder at termination of the Call-Off Contract

Buyer to provide laptops for access to Virtual MODNET to enable the delivery of the service.

Additional quality requirements & standards (in addition to any quality requirements & standards detailed in the addition to the Call-off Schedules)

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

- No specific Quality Management System requirements are defined. This does not relieve the Supplier of providing conforming products under this contract.
- No Deliverable Quality Plan is required reference DEFCON 602B.
- Concessions shall be managed in accordance with Def Stan. 05-061 Part 1, Issue 7 - Quality Assurance Procedural Requirements - Concessions.
- Any contractor working parties shall be provided in accordance with Def Stan. 05-061 Part 4, Issue 4 - Quality Assurance Procedural Requirements - Contractor Working Parties.

## Project and risk management

The Supplier shall appoint a Supplier's Authorised Representative and the Requirement Holder shall appoint a Requirement Holder's Authorised Representative, who unless otherwise stated in this Order Form shall each also act as Project Manager, for the purposes of this Contract through whom the provision of the Services and the Goods shall be managed day-to-day.

Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract. The Supplier shall develop, operate, maintain and amend, as agreed with the Requirement Holder, processes for: (i) the identification and management of risks; (ii) the identification and management of issues; and (iii) monitoring and controlling project plans.

**Timescales** (Prior to Further Competition enter anticipated dates. Following Further Competition update with actual dates)

Call-Off Start Date	22/11/2024
Call-Off Initial Period	5 months
Call-Off Expiry Date	13/04/2025
Call-Off Optional Extension Period	6-months
Minimum notice period prior to a Call-Off Optional Extension Period	1-month's notice

DIPS Order Form / Statement of Requirements Template

(Framework Schedule 6)

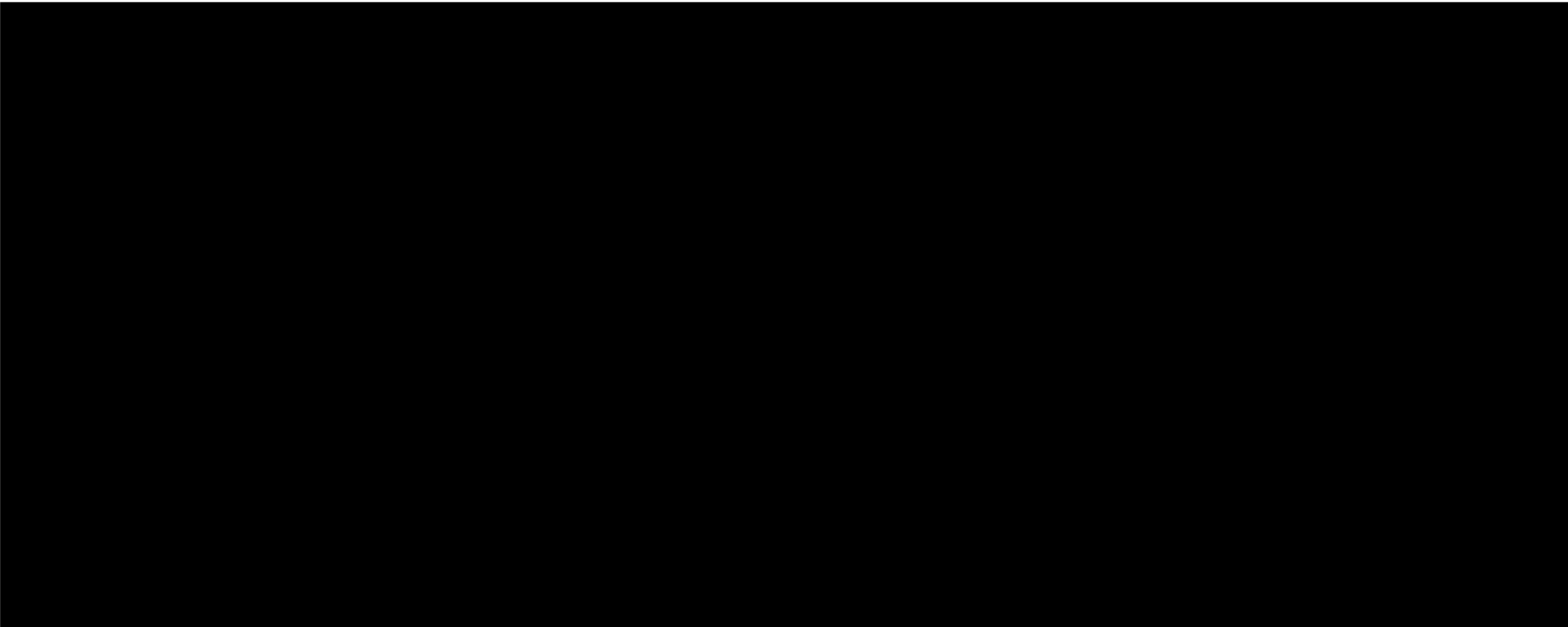
Organisation Role / Position	Dep-Hd CIO Ops	Date	23/05/2024
Approver's signature	<div></div>		

OFFICIAL-SENSITIVE - COMMERCIAL  
OFFICIAL SENSITIVE (when complete)

**DIPS Order Form / Statement of Requirements Template  
(Framework Schedule 6)**

Original FBC Number <i>(when known)</i>	Amendment FBC Number <i>(if applicable)</i>
BMfS Data Catalogue & Reference Data Manager Content Creation V1.0	N/A

OFFICIAL-SENSITIVE - COMMERCIAL



TOTAL: £503,365.00

OFFICIAL SENSITIVE (when complete)





## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

### 2. Call-Off Incorporated Terms

The following documents are incorporated into this Call-Off Contract. Where numbers are missing those schedules are not being used in this Call-Off Contract. If the documents conflict, the following order of precedence applies:

- 1 This Order Form including the General Conditions in section 2(b) and the Call-Off Special Terms in section 2(c).
- 2 Joint Schedule 1 (Definitions)
- 3 Any Statement(s) of Work (in the form of the template set out in Appendix 4 to this Framework Schedule 6 (Order Form Template, Statement of Requirements Template)) executed by the Requirement Holder and the Supplier with a corresponding Call-Off Contract reference
- 4 [Framework Special Terms] No special terms included.
- 5 The following Schedules in equal order of precedence:
  - Joint Schedules ○ Joint Schedule 2 (Variation Form) ○ Joint Schedule 3 (Insurance Requirements) ○ Joint Schedule 4 (Commercially Sensitive Information) ○ Joint Schedule 5 (Corporate Social Responsibility) ○ Joint Schedule 10 (Rectification Plan) ○ Joint Schedule 11 (Processing Data)
  - Call-Off Schedules ○ Call-Off Schedule 3 (Continuous Improvement) ○ Call-Off Schedule 5 (Pricing Details and Expenses Policy) ○ Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) ○ Call-Off Schedule 9 (Security) ○ Call-Off Schedule 10 (Exit Management) ○ Call-Off Schedule 13 (Implementation Plan and Testing) ○ Call-Off Schedule 17 (MOD Terms) ○ Call-Off Schedule 26 (Cyber)
- 6 Core Terms (DIPS version)
- 7 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Requirement Holder (as decided by the Requirement Holder and Commercial) take precedence over the documents above.

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

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

### 2a. Strategy for procurement and evaluation

Further competition	<input checked="" type="checkbox"/>	Competitive award criteria to be used for undertaking evaluation of proposal(s)			
Direct award	<input type="checkbox"/>				
		Weighting (Technical)	55%	Weighting (Price)	45%

### 2b. General Conditions

<b>Additional Conditions:</b> <ul style="list-style-type: none"> <li>The Authority has determined that this contract is a managed service and therefore responsibility for determining the IR35 status and informing resources passes to the supplier.</li> <li>Valid SC Clearance s required as a minimum.</li> </ul>	<input checked="" type="checkbox"/>
--	-------------------------------------

### 2c. Call-Off Special Terms

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

### 2d. Call-Off Charges

Capped Time and Materials (CTM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Incremental Fixed Price	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time and Materials (T&M)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fixed Price	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A combination of two or more of the above Charging methods	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

T&S is applicable	<input checked="" type="checkbox"/>
-------------------	-------------------------------------

£6,000 ex vat T&S Limit of Liability is available for the initial contract period. An additional £6,000 ex vat T&S Liability to be made available if the extension option is to be invoked.

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) and the Supplier shall charge the Requirement Holder a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

**Reimbursable Expenses**

[See Expenses Policy in Annex 1 to Call-Off Schedule 5 (Pricing Details and Expenses Policy)] [None]

### 2e. Payment Method

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

CP&F payment to be attached to delivery of milestone **PO Number TBC**

### Requirement Holder's Invoice Address

Ursula Bishop-Harper  
ODS & DSI Delivery Lead  
07403 858833  
NH3, Cedar 2A,  
MOD Abbeywood  
Bristol  
BS34 8JH

### Requirement Holder's Authorised Representative

[REDACTED]

BmFS Programme Delivery Manager – Enablers

07553 730706

[scott.latham108@mod.gov.uk](mailto:scott.latham108@mod.gov.uk)

NH3, Cedar 2A,  
MOD Abbeywood  
Bristol BS34 8JH

### 2f. Milestone Payments Schedule (MPS) (expand table as appropriate)

Milestone/ Stage Payment number	Key Deliverable (Full details in 1d)	Due Date	%	Milestone Payment value £ (ex VAT)
Mobilisation	As per 1d in Key Deliverables template	22/12/24		
DCCR 1	<b>Data Catalogue Analysis &amp; Design</b> <ul style="list-style-type: none"> <li>Requirements</li> <li>Architecture gap analysis</li> <li>Training requirements</li> <li>MVP high-level design &amp; test strategy</li> </ul>	22/12/2024		
DCCR 2	<b>RDM Planning and MVP design,</b> <ul style="list-style-type: none"> <li>RDM service requirements</li> <li>Architecture gap analysis</li> <li>MVP High level design</li> </ul> Test cases document	22/12/2024		
DCCR 3	<b>Data Catalogue Content Creation MV</b> <ul style="list-style-type: none"> <li>Data catalogue service linked to the data glossary &amp; test cases.</li> <li>Roles and workflow implemented.</li> <li>Document data catalogue service usage</li> </ul> Roadmap for adoption of data catalogue service	22/12/2024		
DCCR 4	<b>RDM setup, configuration and documentation</b> <ul style="list-style-type: none"> <li>Configured reference data master.</li> <li>Document R360 training</li> </ul>	09/02/2025		

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

DCDR 5	<b>Reference data ingestion and planning of next stage</b> <ul style="list-style-type: none"> <li>Deployment plan</li> <li>Test results</li> <li>Knowledge transition</li> </ul>	13/04/2025	
<b>FINAL Payment</b>	Satisfactory delivery and final acceptance of all work in providing the Deliverables. <i>(This final payment should include any costs held as retention based on % of the total cost.)</i>		
Total Contract Value			£503,365.00

### 2g. Maximum Liability

The limitation of the Supplier's liability for this Call-Off Contract is stated in Clause 11.4 of the Core Terms.

### 2h. Requirement Holder's Environmental Policy

Available online at: [Management of environmental protection in defence \(JSP 418\) - GOV.UK \(www.gov.uk\)](#) This version is dated 18<sup>th</sup> August 2023.

### 2i. Requirement Holder's Security Policy

Security Aspects Letter to be issued and executed alongside this Order Form. See Appendix 5.

### 2j. Progress Reports and meetings

Progress Report Frequency	1 per week	Progress Meeting Frequency	Weekly checkpoints
---------------------------	------------	----------------------------	--------------------

### 2k. Quality Assurance Conditions

According to the product or scope of the work to be carried out, the Supplier shall meet the following requirements:

Allied Quality Assurance Publications (AQAP) 2110 – North Atlantic Treaty Organization (NATO) Quality Assurance Requirements for Design, Development and Production.

Certificate of Conformity shall be provided in accordance with DEFCON 627 (*Edn12/10*).

☐

### Deliverable Quality Plan requirements:

DEFCON 602A (*Edn 12/17*) - Quality Assurance with Quality Plan

☐

DEFCON 602B (*Edn 12/06*) - Quality Assurance without Quality Plan

☒

AQAP 2105:2 – NATO Requirements for Deliverable Quality Plans

☐

### Software Quality Assurance requirements

Allied Quality Assurance Publications (AQAP) 2210 – North Atlantic Treaty Organization (NATO) Supplementary Software Quality Assurance Requirements to AQAP-2110 shall apply

☐

### Air Environment Quality Assurance requirements

Defence Standard (DEF STAN) 05-100 – Ministry of Defence Requirements for Certification for Aircraft Flight and Ground Running (Mandatory where flying and/or ground running of issued aircraft is a requirement of the Task)

☐

Relevant MAA Regulatory Publications (See attachment for details)

☐

Additional Quality Requirements (See attachment for details)

☐

### Planned maintenance schedule requirement

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Not Applicable.	<input checked="" type="checkbox"/>
-----------------	-------------------------------------

### 2l. Key Staff

--	--

### 2m. Key Subcontractor(s)

--	--

### 2n. Commercially Sensitive Information

Full Commercial and Technical response	
--	--

### 2o. Cyber Essentials

<p><b>Cyber Essentials Scheme:</b> The Requirement Holder requires the Supplier to have and maintain a Cyber Essentials Plus Certificate for the work undertaken under this Call-Off Contract, in accordance with Call-Off Schedule 26 (Cyber).</p> <p>RAR-240523A08. As the Cyber Risk Profile is Not Applicable no further DCPD action is required.</p>	<input type="checkbox"/>
---	--------------------------

### 2p. Implementation Plan

A high level schedule as to how Supplier will address the SOW will be required.	<input checked="" type="checkbox"/>
---	-------------------------------------

### 3. Charges

Estimated Contract Value (excluding VAT) for Call-Off Contract
Fixed price of £503,365.00 ex VAT, plus £6,000.00 ex VAT T&S Limit of Liability.
Total Contract Value £509,365.00 ex VAT

### 4. Additional Insurances

Not Applicable.
-----------------

### 5. Guarantee

Not applicable.
-----------------

### 6. Social Value Commitment

OFFICIAL SENSITIVE (when  
complete)

## DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The supplier shall meet its Social Value Commitments as described within Call-Off Schedule 4 (Call-Off Tender)

The supplier has committed to the following below:

**To invest 1% of the annual contract revenue towards Social Value.**

### **Lunch and Learns Sharing Best Practice amongst employee-led Diversity Networks**

We know that improving diversity is important to the MOD and we would like to work together with you to improve working practices to promote an inclusive working environment. Twice per year, Team ADA will conduct a best practice sharing session between one of our employee-led Diversity Networks and your equivalent. Enabling and strengthening the employee-led networks has a multiplier effect delivering additional social value across both of our organisations. **KPI 1: Number of Employee Networks participating in knowledge sharing.**

### **Tackling skills shortages driving inequality**

As a member of the Valuable 500 (companies working together to end disability exclusion) we will share learnings by supporting workshops for disadvantaged groups and mentorship programmes using our teams' contract specific volunteering hours of half a day per team member/year (approximately 20 hours/year) to support digital bootcamps, training events and employability workshops. Numeracy is a core skill required for employment. Those from diverse backgrounds more likely to have lower levels of numeracy, creating persistent inequality. Our team, along with your colleagues who would like to, will participate in a National Numeracy Day event, tackling a skills shortage causing inequality in a deprived area important to the military community, such as the Aldershot Park Nepali community. **KPI 2: Number of actions taken to improve skills for disadvantaged groups numeracy.**

### **Supporting those under presented in the workforce**

Support BID Services charity for individuals with sensory impairments, sponsoring digital workshops over 12 months, providing 1:1 training for individuals that suffer from disabilities such as sight impaired, severely sight impaired or blindness – **KPI 3. Number of individuals supported to improve digital literacy.**

### **Project Plan and Process: Governance, Reporting and Transparency**

We now have incorporated Thrive an online dashboard to easily collective qualitative and quantitative data from internal staff and suppliers. Thrive uses the Impact Evaluation Standard (IES) and as such as have tailored our KPIs. Establish SV contract governance, agree measurable KPIs, reporting frequency using the Thrive platform and Impact Evaluation Standards framework, strategies and prioritise commitments and shape the action plan.

		W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21	W22	W23	W24
0) Team ADA x BMFS Social Value Kick Off	Stakeholder engagement, baselining and planning																								
	Social Value Kick Off Session																								
	Establish Team ADA x BMFS SV governance																								
	Inflight Social Value Governance																								
7.1) Sharing Best Practice amongst employee-led Diversity Networks	Ongoing support and interaction with employee-led Diversity Networks																								
	Best Practice Workshop																								
7.2) Tackling Skills Shortages driving inequality	Identify target community & prepare																								
	National Numeracy Day Session																								
7.3 Supporting those under presented in the workforce	Team ADA support to BID services Charity																								

OFFICIAL SENSITIVE (when complete)

**DIPS Order Form / Statement of Requirements Template  
(Framework Schedule 6)**












7. Requirement Holder Commercial Officer Authorisation			
Order Form approved by (Name in capital letters)		Telephone	
Directorate / Division	Defence Digital Professional Services	Email	
Organisation Role / Position	Prof Svcs DD UKStratCom DD-CM- PSCO-02	Date	
Approver's signature			

8. Acknowledgement by Supplier			
Order Form acknowledged by (Name in capital letters)		Telephone	
Supplier Name	KPMG UK	Email	
Supplier Role / Position	DIRECTOR	Date	22/11/2024
Approver's signature			

9. Final Administration	
On receipt of the Order Form acknowledgement from the Supplier, the Commercial Manager (who placed the order) <b>must</b> send an electronic copy of the acknowledged Order Form, together with any applicable Appendix 3 to this Schedule 6, directly to <b>DIPS Professional Services Team</b> at the following email address: <a href="mailto:ukstratcomdd-cm-cct-dips-mail@mod.gov.uk">ukstratcomdd-cm-cct-dips-mail@mod.gov.uk</a>	

OFFICIAL SENSITIVE (when complete)

**Appendix 1 - Addresses and Other Information**

<b>1. Commercial Officer Name:</b> Jessica Walton  Address: MOD Corsham, Westwells Road, Corsham, SN13 9NR  Email: <span style="background-color: black; color: black;">[REDACTED]</span>  	<b>8. Public Accounting Authority</b>  1. Returns under DEFCON 694 (or SC equivalent) should be sent to DBS Finance ADMT – Assets In Industry 1, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD  44 (0) 161 233 5397  2. For all other enquiries contact DES Fin FA-AMET Policy, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD  44 (0) 161 233 5394
<b>2. Project Manager, Equipment Support Manager or PT Leader</b> (from whom technical information is available) Name:  Address   Email:  	<b>9. Consignment Instructions</b> The items are to be consigned as follows:
<b>3. Packaging Design Authority Organisation</b> & point of contact:  (Where no address is shown please contact the Project Team in Box 2)  	<b>10. Transport.</b> The appropriate Ministry of Defence Transport Offices are: <b>A. DSCOM.</b> DE&S, DSCOM, MoD Abbey Wood, Cedar 3c, Mail Point 3351, BRISTOL BS34 8JH <u>Air Freight Centre</u> IMPORTS  030 679 81113 / 81114 Fax 0117 913 8943 EXPORTS  030 679 81113 / 81114 Fax 0117 913 8943 <u>Surface Freight Centre</u> IMPORTS  030 679 81129 / 81133 / 81138 Fax 0117 913 8946 EXPORTS  030 679 81129 / 81133 / 81138 Fax 0117 913 8946 <b>B. JSCS</b>  JSCS Helpdesk No. 01869 256052 (select option 2, then option 3) JSCS Fax No. 01869 256837 Users requiring an account to use the MOD Freight Collection Service should contact <a href="mailto:UKStratCom-DefSp-RAMP@mod.gov.uk">UKStratCom-DefSp-RAMP@mod.gov.uk</a> in the first instance.
<b>4. (a) Supply / Support Management Branch or Order Manager:</b> <b>Branch/Name:</b>    <b>(b) U.I.N.</b>	
<b>5. Drawings/Specifications are available from</b>	<b>11. The Invoice Paying Authority</b> Ministry of Defence  0151-242-2000 DBS Finance Walker House, Exchange Flags Fax: 0151-242-2809 Liverpool, L2 3YL <b>Website is:</b> <a href="https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement">https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement</a>
<b>6. Intentionally Blank</b>	<b>12. Forms and Documentation are available through *:</b> Ministry of Defence, Forms and Pubs Commodity Management PO Box 2, Building C16, C Site Lower Arncott Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824) <b>Applications via fax or email:</b> <a href="mailto:Leidos-FormsPublications@teamleidos.mod.uk">Leidos-FormsPublications@teamleidos.mod.uk</a>

<p><b>7. Quality Assurance Representative:</b></p> <p>Commercial staff are reminded that all Quality Assurance requirements should be listed under the General Contract Conditions.</p> <p><b>AQAPS</b> and <b>DEF STANs</b> are available from UK Defence Standardization, for access to the documents and details of the</p>	<p><b>* NOTE</b></p> <p>1. Many <b>DEFCONs</b> and <b>DEFFORMs</b> can be obtained from the MOD Internet Site: <a href="https://www.kid.mod.uk/maincontent/business/commercial/index.htm">https://www.kid.mod.uk/maincontent/business/commercial/index.htm</a></p>
--	--

helpdesk visit <http://dstan.gateway.is>OFFICIALg-

[r.r.mil.uk/index.htm](http://r.r.mil.uk/index.htm) L-SENSITIVE

[intranet] or <https://www.dstan.mod.uk/> [extranet, registration needed].

- COMMERCIAL SENSITIVE INFORMATION -  
The required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.

**OFFICIAL SENSITIVE (when complete)**

13

**OFFICIAL SENSITIVE (when complete)**

14

OFFICIAL-SENSITIVE - COMMERCIAL-SENSITIVE - COMMERCIAL

Framework Schedule 6 (Order Form Template, Statement of Requirements Template)

Appendix 2 to Schedule 6

## Appendix 2 – Supplier's Quotation - Charges Summary

## Framework Schedule 6 (Order Form Template, Statement of Requirements Template)

1. To:

2. From:

KPMG UK

Date of tender submission: 2  
October 2024

In response to the Order Form request for a quotation  
reference

Dated: x  
November 2024

\*The work can be undertaken and our detailed response is attached ☒

\*We are unable to provide the resources/deliverables identified on this occasion. ☐  
(Check box as appropriate)

Name: (Block Capitals)

Signed:

Date:

2. Call-Off title: RM6249

3. Supplier Unique Reference Number:

4. Start Date: 18 November 2024

Completion Date: 30  
April 2025

## 5a. Manpower/Resources

Broad Capability Area Number	Grade	Daily rate quoted at ITT	Daily rate quoted for this task	Reduction on original ITT rate	No of Days	Total

## 5b. Travel

(Estimated expenditure on:)

Unit cost

Number of  
Journeys / Miles

Total

Rail

Motor Mileage  
(max 30p per mile incl VAT)30p max  
(incl VAT)

Air

Sea

## 5c. Subsistence

(Estimated expenditure on:)

Unit cost

Number of  
Night / Days

Total

Accommodation  
(max £100 per night incl VAT)Meals (max £5 for lunch and/or  
£22.50 for an evening meal,  
including all drinks)Miscellaneous costs (please  
define below)

The above T&amp;S costs relate to the period to

## Framework Schedule 6 (Order Form Template, Statement of Requirements Template)

**Subcontractor price**

### 5d. Other Costs

## Subcontractor Details

## Materials

Other

(Please provide details below)

### Description

Cost

...£503,365.00.... (excl. VAT)

### Total Charges for completion of Call-Off Contract

## Deliverables

Framework Schedule 6 (Order Form Template, Statement of Requirements Template)

## Appendix 3 (Statement of Work)

### 1. Statement of Work (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below). All capitalised terms in this SOW shall have the meanings set out in Joint Schedule 1 (Definitions) unless otherwise stated.

The Parties may execute a SOW for any set of Deliverables required. For any ad-hoc Deliverables requirements, the Parties may agree and execute a separate SOW, or alternatively agree a Variation to an existing SOW.

All SOWs must fall within the Specification and provisions of the Call-Off Contract.

The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.

**Date of SOW:** 30<sup>th</sup> October 2024

**SOW Title:** BMfS Data Catalogue & Reference Data

**SOW Reference:** SOW1

**Call-Off Contract Reference:** RM6249/DIPS(1)034

**Requirement Holder:** [REDACTED]

**Supplier:** KPMG

**SOW Start Date:** 22<sup>nd</sup> November 2024

**SOW End Date:** 13<sup>th</sup> April 2025

**Duration of SOW:** 5 months

**Key Personnel (Requirement Holder):** [REDACTED]

**Key Personnel (Supplier):** [REDACTED]

**Subcontractors:** [REDACTED]

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

## 2. Call-Off Contract Specification – Deliverables Context

**SOW Deliverables Background:** The partner is required to source and load DefSp metadata content into the Informatica Cloud Native Data Catalogue service, design and configure the Informatica R360 Reference Data Management service, source and load Reference Data records into the Reference Data Management service, and implement Reference Data Management procedures.

### Delivery phase(s):

#### Discovery phase

Data catalogue analysis activities (DCDR1):

- Agree ways of working, execute planning and requirements workshops.
- Create communication plans with key consumers of DefSupport data (CDO, FLCs, BMfS team and wider MOD Data teams).
- Facilitate workshops between the domains and communities using SDW data.
- Document requirements from the key stakeholders and consumers.
- Conduct gap analysis of current architecture and identify implementation issues.
- Agree prioritised list of data sets and attributes to be delivered.
- Agree and prioritise MVP use case, deliverables, and timelines.
- Agree prioritised SDW data sources for the capture of metadata.
- Define the interaction of the Data Catalogue service with the existing data governance and highlight any gaps.
- Document the critical data entities and attributes for SDW.
- Analyse and document business glossary and data lineage curation needs.
- Check Informatica Out of the box Catalogue connectors for SDW.
- Document anticipated volumes and metrics per data domain for each platform.
- Document training and workshop needs for MOD stakeholders.

#### RDM analysis activities (DCDR2):

- Facilitate stakeholder workshops to understand the goals for reference data management.
- Document business objectives, the current technical landscape, challenges, existing reference data sets and their owners.
- Document 'as is' business context and legacy systems involving reference data and processes.
- Analyse and identify the data sources for use cases.
- Document enterprise architecture requirements for RDM solution, with the integration points and any customisation needs.
- Document reference data consumption systems requirements.
- Document the MVP criteria for R360 SaaS and integration touch points.

#### Data catalogue design activities (DCDR1):

- Implement HLD and configure the CDGC to crawl the SDW database to get the metadata for in scope items.
- Tag the relevant data, curate it to create the data catalogue and link to data glossary linking and create data lineage for the identified Critical data elements.
- Implement workflows and onboard users with relevant access rights.
- Capture risk, challenges with data set ingestion and identify any dependencies for consuming systems.
- Define the governance roles and responsibilities of stakeholders such as data owners and data stewards into RACI matrix.
- In partnership with the DD CDO design and provide training to data consumers to exploit the catalogue service, focussing on priority use cases.
- Agree a future plan and roadmap, for creating data catalogue entries for all BMfS in-scope applications.

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

**RDM design activities (DCDR2):**

- Document understanding of 'as is' business context and legacy systems involving reference data and the processes.
- Profile the data sources for reference data and identify the potential issues.
- Document the agreed MVP criteria for R360 SaaS and integration touch points.
- Map the usage patterns and requirements to data reference architecture.
- Design MVP RDM Architecture and the integration points.
- Customise the data reference architecture and solution alternatives definition to fit MOD requirements.
- Finalise reference architecture on recommended data platform.
- Design data model and data preparation for the reference dataset identified for MVP.
- Document RDM roles and responsibilities.
- Document RDM workflows.

**MVP execution & implementation****Data Catalogue build and implement activities (DCDR3):**

We will conduct the following:

- Based on the High-Level Design create a catalogue of the applications, categorised by line of businesses or technologies.
- Document and capture the complexity of integration and any customisation required.
- Document the dependency between the SDW related systems.
- Configure the Out Of The Box (OOTB) connector and import metadata assets based on scope from the Discovery Phase.
- Implement the configuration of the roles and responsibilities for data stewards & owners based on the scope from the Discovery Phase.
- Implement the metadata for prioritised data attributes in the Informatica Data Catalogue, including an example of de-conflicting definitions and data lineage.
- Catalogue the agreed attributes from the SDW and provide access to users.
- Link metadata to glossary.
- Define how new users gain access to the catalogue in conjunction with CDO teams.
- Agree the plan and roadmap for scaling the MVP to ingest other source metadata within the BMfS programme.

**RDM build and implement activities (DCDR4):**

- Work with MOD Defense Digital team for platform setup and configuration for RDM.
- Work with MOD IT team for Cognizant R360 accelerator setup.
- Integrate with role based SSO authentication methods.
- Document reference data onboarding steps and FAQs.
- Document processes and training for users.
- Import code values for identified MVP scope and prepare code list and codes-values
- Implement business rules/validation rules.
- Configure reference datasets, crosswalks.
- Configure hierarchies within the reference data.
- Configure roles and workflows for reference data management.
- Configure out of the box UI.
- Conduct a "show and tell" session with the data stewardship team.
- Publish the reference data to outbound system.

**Data Catalogue testing activities (DCDR3):**

We will conduct the following:

- Validation of metadata scanning, data model.
- Validation of classification, tagging, profiling.
- Validation of business glossary, data lineage.
- Validation of policies, workflows.

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

- Provide UAT support for MVP testing.

#### **RDM testing activities (DCDR4):** We

will conduct the following:

- Validation of RDM data model, table structure against the specifications.
- Validation of code lists, code lists, hierarchies.
- Validation of MVP data ingestion from source to Informatica R360.
- Validation of incremental data loads.
- Validation of de normalised reference data load in data lake.
- Validation of data integrity, business rules and workflows implemented.
- Provide UAT support for MVP testing.

#### **Extended Implementation**

#### **Reference data ingestion & planning of next stage (DCDR5):** We

will conduct the following:

- Demonstrations of MVP capability.
- Working sessions on the use of IR360 to support and sustain work delivered.
- Secure formal sign off.
- Planning for next stage of RDM and data catalogue.

#### **Overview of Requirement:**

The Business Modernisation for Support (BMfS) Programme has the ambitious goal of modernising and replacing the legacy business processes and technology systems that deliver the MOD's critical support chain. The project goal is to load DefSp metadata content into the Informatica Data Catalogue service, design and configure the Informatica R360 Reference Data Management service, source and load Reference Data records into the Reference Data Management service and implement Reference Data Management procedures.

The establishment of the BMfS data catalogue and reference data management service are core components in the successful delivery of BMfS Programme.

When providing the Services, the Supplier will not perform any management functions, nor make any decisions for the Buyer, and while the Supplier may provide the Buyer with advice, responsibility for all related decisions and their consequences are the Buyer's responsibility. The Buyer must appoint someone of management-level with the skill, knowledge and experience necessary to be responsible for overseeing the Services provided, evaluating their adequacy, establishing and maintaining internal controls and monitoring ongoing activities.

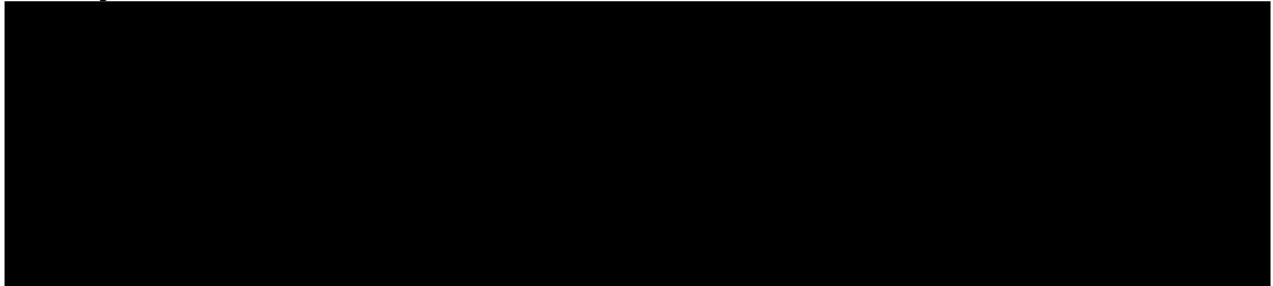
### **3. Requirement Holder Requirements – SOW Deliverables**

#### **Outcome Description:**

<b>Milestone Ref</b>	<b>Milestone Description</b>	<b>Acceptance Criteria</b>	<b>Due Date</b>
MS01	DCDR1: Data Catalogue Analysis & Design (MVP defined)	Finalised MVP Scope HLD signoff Approval	22/12/2024
MS02	DCDR2: MVP delivered. A joint review of the MVP requirement set	Finalised RDM Scope MVP plan signoff Approval	22/12/2024

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

MS03	DCCR3: Catalogue content creation; delivery of application group 2.	Objective: Delivery Phase (15 weeks)  Metadata acquisition CDGC Configurations complete Data catalogue and lineage complete MVP Testing completion User demos, Create CGDC Roadmap, MVP complete. Future adoption plan and Roadmap R360 MVP Integrations complete R360 MVP Testing complete. R360 MVP User demos, MVP complete Future adoption plan and Roadmap	22/12/2024
MS04	DCCR4: Catalogue content creation; delivery of application group 3.	R360 Setup R360 MVP configurations complete R360 Ready for use	13/04/2025
MS05	DCCR5: Reference data ingestion and planning of next stage	Demonstrations of MVP capability.  Planning for next stage of RDM and data catalogue. Working sessions on the use of IR360 to support and sustain work delivered.  Secure formal sign off.	09/02/2025

**Delivery Plan:****Dependencies:**

- Informatica licenses and costs for the data catalogue and reference data management are provided by MOD.
- Access to MOD SMEs and data sources
- Licence and third-party vendor costs will be covered by MOD.
- Data catalogue and RDM instances for dev, test, prod.
- Administer user access setup, environment setup, VPN setup.
- Provide sample data sets in Dev/Pilot instances.
- Help define the prioritisation of key data attributes.
- Access to infrastructure/ environment & documents for MVP testing.

**Supplier Resource Plan:**

Resource	Applied to Role	Project Stage	Expertise & Knowledge
Engagement Leader	• Delivery accountability Single point of contact	Throughout	• MOD and Defence Support delivery experience

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

	for the delivery team and client for any escalations or scope.		<ul style="list-style-type: none"> <li>P3M</li> </ul>
Engagement Manager	<ul style="list-style-type: none"> <li>Responsible for MVP Managing plan, scope, and budget</li> <li>Reporting RAIDO</li> </ul>	Throughout	<ul style="list-style-type: none"> <li>MOD and data management delivery</li> <li>experience P3M</li> </ul>
Scrum Master	<ul style="list-style-type: none"> <li>Direct team</li> <li>Planning</li> <li>Workshops</li> <li>Communications</li> <li>QA documentation</li> <li>Resolve barriers</li> </ul>	Throughout	<ul style="list-style-type: none"> <li>Certified SCRUM Master</li> <li>Previous BMfS Programme exp.</li> <li>Data management delivery exp.</li> </ul>
Data Governance Architect	<ul style="list-style-type: none"> <li>Data catalogue requirements</li> <li>Data governance</li> <li>Use cases</li> <li>Service needs</li> <li>Metadata ingestion</li> <li>Implement roles and responsibilities.</li> <li>Ingest SDW data elements in CDGC</li> </ul>	Throughout	<ul style="list-style-type: none"> <li>Certified Informatica architect</li> <li>Informatica CDGC skill</li> <li>Previous design and delivery experience using Informatica</li> <li>Previous BMfS Programme exp.</li> </ul>
Metadata Engineer	<ul style="list-style-type: none"> <li>Configure the data catalogue in CDGC</li> <li>Link data glossary &amp; publish for discovery.</li> <li>Extract data &amp; create metadata on CDGC for prioritised CDEs</li> <li>Work with DG Architect to setup roles and responsibilities</li> <li>Action SDW metadata into CDGC</li> </ul>	Design, Build, SIT, UAT	<ul style="list-style-type: none"> <li>Informatica CDGC skill</li> <li>Previous MOD data engineering exp</li> </ul>
Business Analyst	<ul style="list-style-type: none"> <li>Define data catalogue, reference data, &amp; RDM architecture requirements</li> <li>Conduct gap analysis workshops</li> <li>Process mapping, usecase election, key data element identification</li> <li>Create business and DQ rules</li> <li>Document glossary</li> <li>Requirements for management dashboards</li> </ul>	Analysis & design	<ul style="list-style-type: none"> <li>Good understanding on RDM</li> <li>Previous exp in documenting requirements</li> </ul>

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Data Analyst	<ul style="list-style-type: none"> <li>• Profile data</li> <li>• Discover DQ rules</li> <li>• Analyse data dependencies</li> <li>• Code lists &amp; metadata from CDGC</li> <li>• Crosswalk requirements</li> <li>• Identify logic to create</li> </ul>	Analysis & design	<ul style="list-style-type: none"> <li>• Good understanding on DQ/DG</li> <li>• Previous exp in data analysis including data profiling and pattern analysis</li> </ul>
	<ul style="list-style-type: none"> <li>• unique R360 keys</li> <li>• Create data catalogue and RDM design</li> </ul>		
QA Engineer	<ul style="list-style-type: none"> <li>• Create test plans</li> <li>• Execute tests</li> <li>• Create/delete/update data in existing code list and approval workflows</li> <li>• Identify parent-child dependencies, Validate MVP outcomes</li> </ul>	Design, Build, SIT, UAT	<ul style="list-style-type: none"> <li>• Proficiency in manual/automated data testing techniques</li> <li>• Good understanding on SQL and DQ/DG</li> <li>• Previous exp in DQ/DG</li> </ul>
RDM Architect	<ul style="list-style-type: none"> <li>• Conduct RDM service workshops</li> <li>• Understand existing RDM</li> <li>• Map RDM to the R360 (features and functionality)</li> <li>• Setup R360 service.</li> <li>• Configure the service with integration to ingest and publish reference data.</li> <li>• Evaluate MVP outcomes</li> </ul>	Throughout	<ul style="list-style-type: none"> <li>• R360 Platform proficiency</li> <li>• Exp in DQ/DG/RDM</li> <li>• Previous design and delivery experience using R360.</li> </ul>
AWS/IICS Developers for RDM	<ul style="list-style-type: none"> <li>• Design and build workflows to integrate data from sources.</li> <li>• Create processing jobs to extract, transform and load the data into R360</li> </ul>	Design, Build, SIT, UAT	<ul style="list-style-type: none"> <li>• Certification in AWS/IICS/Data Management</li> <li>• Exp in DQ/DG/RDM/ETL/SQL/RDM</li> </ul>
RDM Developer	<ul style="list-style-type: none"> <li>• Setup governance roles in R360</li> <li>• Setup 2 step approval workflows with roles such as approver/reviewer and action comment type.</li> <li>• Setup taxonomy of data, audit trail and build and configure R360 components reference data, code lists, crosswalks and hierarchies for MVP</li> <li>•</li> </ul>	Design, Build, SIT, UAT	<ul style="list-style-type: none"> <li>• Certification in Data Management</li> <li>• Understanding of RDM /DQ/DG concepts</li> <li>• Experience in configuration and customisation in R360</li> </ul>

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

	Build and validate R360 for MVP.		
--	----------------------------------	--	--

**Security Applicable to SOW:**

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Holder Systems and Deliverables with completed Supplier staff vetting at SC Level.

**SOW Standards:**

Delivery will be conducted in line with standards set out in the Order Form

**Performance Management:**

Not applicable.

**Additional Requirements:**

**Annex 1** – Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex 1 attached to this Statement of Work.

**Key Supplier Staff:**

Key Role	Key Staff
Engagement Leader	
Engagement Manager	
Delivery Manager	
Business Analyst	

**SOW Reporting Requirements:**

Further to the Supplier providing the management information specified in Framework Schedule 5 (Management Charges and Information), the Supplier shall also provide the following additional management information under and applicable to this SOW only:

Ref.	Type of Information	Which Deliverables does this requirement apply to?	Required Submission	regularity	of
1.					
1.1	Status report	All	Weekly		

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

#### 4. Charges

##### Call Off Contract Charges:

The applicable charging method(s) for this SOW is:

- Fixed Price

The maximum value of this SOW (irrespective of the selected charging method) is **£503,365.00 ex VAT**

##### Reimbursable Expenses:

See Expenses Policy in Annex 1 to Call-Off Schedule 5 (Pricing Details and Expenses Policy)

Reimbursable Expenses are capped at **£6,000.00** of the Charges payable under this Statement of Work.

Should the extension option be executed, then the Reimbursable Expenses for the additional 6month period will also be capped at **£6,000.00**.

#### 5. Signatures and Approvals

##### Agreement of this SOW

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 3 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

##### For and on behalf of the Supplier

Name: [REDACTED]

Title: Director

Date:

Signature:

##### For and on behalf of the Requirement Holder

Name: [REDACTED]

Title: BMfS Programme Delivery Manager Date:

Signature:

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

## Annex 1 to Statement of Work

### Data Processing – N/A

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

[Template Annex 1 of Joint Schedule 11 (Processing Data) Below]

Description	Details
Identity of Controller for each Category of Personal Data	<p><b>The Relevant Authority is Controller and the Supplier is Processor</b></p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 of Joint Schedule 11 (Processing Data) and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> <li>• [Insert the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority]</li> </ul> <p><b>The Supplier is Controller and the Relevant Authority is Processor</b></p> <p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of Joint Schedule 11 (Processing Data) of the following Personal Data:</p> <ul style="list-style-type: none"> <li>• [Insert the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier]</li> </ul> <p><b>The Parties are Joint Controllers</b></p> <p>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> <li>• [Insert the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]</li> </ul> <p><b>The Parties are Independent Controllers of Personal Data</b></p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> <li>• Business contact details of Supplier Personnel for which the Supplier is the Controller,</li> <li>• Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which</li> </ul>

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

	<p>the Relevant Authority is the Controller,</p> <ul style="list-style-type: none"> <li>• <b>[Insert</b> the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority]</li> </ul> <p><b>[Guidance</b> where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]</p>
Duration of the Processing	[Clearly set out the duration of the Processing including dates]
Nature and purposes of the Processing	<p>[Be as specific as possible, but make sure that you cover all intended purposes.</p> <p>The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]</p>
Type of Personal Data	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]
Categories of Data Subject	[Examples include: Personnel (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.]

## Appendix 5 - Confidentiality Undertaking

**[Requirement Holder guidance:** Appendix 5 is for use where required pursuant to clause 15.3 of the Core Terms]

Employee:

Name of Employer:

MOD Contract/Task No:

Title:

1. I, the above named employee, confirm that I am fully aware that, as part of my duties with my Employer in performing the above-named Contract, I shall receive confidential information of a

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules) sensitive nature (which may include particularly commercially sensitive information), whether documentary, electronic, aural or in any other form, belonging to or controlled by the Secretary of State for Defence or third parties. I may also become aware, as a result of my work in connection with the Contract, of other information concerning the business of the Secretary of State for Defence or third parties, which is by its nature confidential.

2. I am aware that I should not use or copy for purposes other than assisting my Employer in carrying out the Contract, or disclose to any person not authorised to receive the same, any information mentioned in paragraph 1 unless my Employer (whether through me or by alternative means) has obtained the consent of the Secretary of State for Defence. I understand that "disclose", in this context, includes informing other employees of my Employer who are not entitled to receive the information.

3. Unless otherwise instructed by my Employer, if I have in the course of my employment received documents, software or other materials from the Secretary of State for Defence or other third party for the purposes of my duties under the above Contract then I shall promptly return them to the Secretary of State for Defence or third party (as the case may be) at the completion of the Contract via a representative of my Employer who is an authorised point of contact under the Contract and (in the case of information referred to under paragraph 1 above) is also authorised under paragraph 2. Alternatively, at the option of the Secretary of State for Defence or the third party concerned, I shall arrange for their proper destruction and notify the above authorised point of contact under the Contract to supply a certificate of destruction to the Secretary of State for Defence. Where my

Employer may legitimately retain materials to which this paragraph applies after the end of the Contract, I shall notify the authorised representative of my Employer to ensure that they are stored, and access is controlled in accordance with my Employer's rules concerning third party confidential information.

4. I understand that any failure on my part to adhere to my obligations in respect of confidentiality may render me subject to disciplinary measures under the terms of my employment.

Signed:

Date:

**Appendix 5 - Security Aspects Letter**

Ministry  
of Defence

C4ISR  
Strategic Command  
Defence Digital  
Mustang 1st Floor  
Westwells Road  
Corsham, SN13 9NR  
Telephone: 03001510271

File reference: PS456

Insert Date: 19/08/2024

For the attention of: KPMG

**PS456 BMfS Data Catalogue and Reference Data Management Content Creation**

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced ITT that constitute classified material.
2. Aspects that constitute 'SECRET Matter' for the purpose of the DEFCON 659A Security Clause and OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
Statement of work	Official Sensitive Commercial
Industry proposals in response	Commercial in Confidence
Existence of a Secret project	Official Sensitive
Secret project names	Official
Full set of Low-Level Design documentation	Secret
Asset (hardware and software) identification for secret systems	Secret
Complete System Installation and configuration documentation for secret systems	Secret
Qualification/System Acceptance Test data (generated for test purposes only) for secret systems	Secret
Test Environment	Secret UKEO
Operational Environment	Secret UKEO

3. Your attention is drawn to the provisions of the Official Secrets Act 1989 and the National Security Act 2023. In particular you should take all reasonable steps to make sure that all individuals employed on any work in connection with this ITT have notice of the above

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules) specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply should the ITT be unsuccessful.

4. Will you please confirm that:

- a. This definition of the classified aspects of the referenced Invitation to Tender has been brought to the attention of the person directly responsible for security of classified material.
- b. The definition is fully understood.
- c. Measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. [The requirement and obligations set out above and in any contractual document can and will be met and that the classified material shall be protected in accordance with applicable national laws and regulations.]
- d. All employees of the company who will have access to classified material have either signed an OSA/NSA Declaration Form in duplicate and one copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA/NSA apply to all classified information and assets associated with this ITT.

- 5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.
- 6. Classified Information associated with this ITT must not be published or communicated to anyone without the approval of the MOD Contracting Authority.
- 7. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Security Officer (PSyO) in accordance with DEFCON 76.
- 8. If you require access to information or assets classified SECRET or above at the tender stage you must provide the MOD Contracting Authority with the personal details of the other members of your company to whom you need to disclose information classified SECRET or above in order to complete your Tender. The number of such other individuals should be restricted to the fewest possible, and they should not in any case be allowed access to information or assets classified SECRET or above until they have been granted the appropriate security clearances.
- 9. Contact details for the MOD Project Security Officer (PSyO) (responsible for the co-ordination of effective security measures throughout the Project/Programme) are included below:

Yours faithfully

Copy via email to:

[ISAC-Group \(MULTIUSER\)](#)  
[COO-DSR-IIPCSy \(MULTIUSER\)](#)  
[UKStratComDD-CyDR-CySAAS-021](#)

Appendix 1  
 To Security Aspect Letter  
 Dated 05 July 24

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

## **UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS**

### **Purpose**

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

### **Definitions**

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

### **Security Grading**

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

### **Security Conditions**

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

### **Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material**

6. The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.
7. Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to comply with the accreditation requirements specified in ISNs 2017/01, 04 and 06, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

<https://www.gov.uk/government/publications/industry-security-notice-isns>. <http://dstan.gateway.isg-r.r.mil.uk/standards/defstans/05/138/000002000.pdf> <https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down>

8. All UK classified material including documents, media and other assets must be physically secured to prevent unauthorised access. When not in use UK classified material shall be handled with care to prevent

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be controlled.

9. Disclosure of UK classified material must be strictly controlled in accordance with the *"need to know"* principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or sub-Contractor.
10. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any classified material issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 8 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.
11. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.
12. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 34.

#### Access

13. Access to UK classified material shall be confined to those individuals who have a *"need-to-know"*, have been made aware of the requirement to protect the material and whose access is essential for the purpose of their duties.
14. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE material have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/714002/HMG\\_Baseline\\_Personnel\\_Security\\_Standard\\_-\\_May\\_2018.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf)

#### Hard Copy Distribution

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

#### Electronic Communication and Telephony and Facsimile Services

17. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules) approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation are available at:

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

Details of the CPA scheme are available at:

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

18. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the information.
19. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so.
20. UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

## Use of Information Systems

21. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.
  22. The Contractor should ensure **10 Steps to Cyber Security** (Link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure competent personnel apply 10 Steps to Cyber Security.
- <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.
23. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.
  24. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK OFFICIAL-SENSITIVE information on IT systems.
    - a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “*least privilege*” will be applied to System Administrators. Users of the IT System (Administrators) should not conduct ‘standard’ User functions using their privileged accounts.
    - b. Identification and Authentication (ID&A). All systems are to have the following functionality:
      - (1). Up-to-date lists of authorised users.
      - (2). Positive identification of all users at the start of each processing session.

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

- c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be “*strong*” using an appropriate method to achieve this, e.g. including numeric and “*special*” characters (if permitted by the system) as well as alphabetic characters.
- d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.
- e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 17 above.
- f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

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

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

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

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

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

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

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

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

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

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

- i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.
- j. Internet Connections. Computer systems must not be connected direct to the Internet or “*un-trusted*” systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).
- k. Disposal. Before IT storage media (e.g. disks) are disposed of, an erasure product must be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

## Laptops

- 25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 17 above.
- 26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites<sup>1</sup>. For the avoidance of doubt the term “*drives*” includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.
- 27. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.
- 28. Portable CIS devices holding the Authorities’ data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

## Loss and Incident Reporting

- 29. The Contractor shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes MOD Identifiable Information (MODDII) (as defined in ISN2016/05) and any information or asset that has been given a security classification by the UK MOD. The term also includes classified information and assets held by UK Defence Contractors which are owned by a third party e.g. NATO or a another country for which the UK MOD is responsible.
- 30. In addition any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD’s Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD Defence Industry WARP will also advise the Contractor what further action is required to be undertaken.

### **UK MOD Defence Industry WARP Contact Details**

**Email:** [DefenceWARP@mod.gov.uk](mailto:DefenceWARP@mod.gov.uk) (OFFICIAL with no NTK restrictions)

**RLI Email:** [defencewarp@modnet.rli.uk](mailto:defencewarp@modnet.rli.uk) (MULTIUSER)

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

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

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

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

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

### Sub-Contracts

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

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

[ISN 2022-08 Subcontracting or Collaborating on Classified MOD Programmes.pdf](https://publishing.service.gov.uk/ISN_2022-08_Subcontracting_or_Collaborating_on_Classified_MOD_Programmes.pdf)  
([publishing.service.gov.uk](https://publishing.service.gov.uk/))

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

### Physical Destruction

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

### Private Venture Activities

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

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

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

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

### Publicity Material

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

37. Contractors wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government.
38. For UK Contractors where the exhibition assets relate to multiple Delivery Teams or for Private Venture defence related material where there is no defined Delivery Team, the Contractor shall request clearance for exhibition from the Directorate of Security and Resilience when it concerns Defence Related Material. See the MOD Exhibition Guidance on the following website for further information:

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

### Export sales/promotion

39. The MOD Form 680 (F680) security procedure enables HMG to control when, how, and if defence related classified material is released by UK Contractors to foreign entities for the purposes of promotion or sales of equipment or services. Before undertaking any targeted promotion or demonstration or entering into any contractual commitments involving the sale or release of defence equipment, information or technology classified UK OFFICIAL-SENSITIVE or above to a foreign entity, a UK Contractor shall obtain F680 approval from the Export Control Joint Unit (ECJU) MOD Team. This includes assets classified UK OFFICIAL-SENSITIVE or above either developed to meet a UK MOD requirement or Private Venture (PV) equipment, as formally advised in a Security Aspects Letter (SAL) issued by the relevant Contracting Authority, or PV Security Grading issued by the MOD Directorate of Security and Resilience. Guidance regarding the F680 procedure issued by ECJU can be found at:

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

40. If a Contractor has received an approval to sub-contract, under an MOD Form 1686 (F1686), for development/production of parts of an equipment, that approval also permits the production of additional quantities for supply to an export customer, when the Contractor has MOD Form 680 approval for supply of the complete equipment, as long as:
- they are identical, except for component obsolescence, to items produced under the UK programme that the approval to subcontract relates to; and
  - no additional OFFICIAL-SENSITIVE or above material is required to be released to the overseas subcontractor.

### Interpretation/Guidance

41. Advice regarding the interpretation of the above requirements should be sought from the Authority.
42. Further requirements, advice and guidance for the protection of UK classified material at the level of UK OFFICIAL and UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

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

### Audit

43. Where considered necessary by the Authority the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractor's processes and facilities by

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)  
representatives of the Contractor's National/Designated Security Authorities or the Authority to ensure  
compliance with these requirements.

**OFFICIAL-SENSITIVE COMMERCIAL****Appendix 6 - Statement of Requirements****BMfS Data Catalogue & Reference Data Management Content Creation SOR****Introduction****Purpose**

The Defence Support (DefSp) function within Ministry of Defence (MOD) Strategic Command has embarked on a Business Modernisation for Support (BMfS) programme to mobilise the best of existing systems, in conjunction with new COTS products and redesigned processes, to substantially improve current support capabilities.

**Background**

The Authority wishes to use its existing data cataloguing and reference data management services provided by Informatica to support the delivery of the objectives below.

**OFFICIAL-SENSITIVE COMMERCIAL****Objectives**

The partner is required to source and load DefSp metadata content into the Informatica Cloud Native Data Catalogue service, design and configure the Informatica R360 Reference Data Management service, source and load Reference Data records into the Reference Data Management service, and implement Reference Data Management procedures.

The partner will be expected to;

- Identify volume and support the ingestion of an agreed subset of data attributes from the (Oracle Stack) Support Data Warehouse (SDW), and priority application services, into the central Defence Informatica Data Catalogue.
- Identify and review priorities for Reference data required by two high priority projects in the BMfS programme (DEEAMS and DFMS).
- Review Master Data Catalogue & Data Modelling work undertaken by DefSp to identify Reference data sets and values.
- Setup and Configure Data Quality rules for profiling Reference data in R360.
- SDW/application data attributes are to be sourced and loaded into the Informatica Data Catalogue solution incrementally on a dataset/sub-domain basis.
- Source and load additional metadata elements for Support Data attributes into the Informatica Data Catalogue.
- Link data records in the informatica Data Catalogue to the correct Data Glossary entries.
- Develop data lineage records in the Catalogue for agreed critical data elements within the SDW.
- Establish the team's ways of working, execution of appropriate discovery workshops, and establishing communication checkpoints to support the achievement of objectives.
- Engage with key stakeholders of SDW datasets to understand and document Data Catalogue consumer requirements.
- Engage with the Defence Digital (DD) Chief Data Office (CDO) regarding the consistent adoption of the Informatica Data Catalogue and Reference Data Management services at scale within Defence. Support the design and implementation of "Data Office Services" relating to Reference Data Management.

**OFFICIAL-SENSITIVE COMMERCIAL**

- Create and communicate a roadmap for the exploitation of the Data Catalogue service within DefSp and wider organisations exploiting DefSp data.
- Undertake a discovery and profiling of DefSp Reference Data elements and define the reference data model to be implemented in the Reference Data Management service for wider consumption.
- Analyse and recommend a migration strategy for existing reference data sets into the Reference Data Management service.
- Design Reference Data stewardship processes for on-going reference data CRUD (Create, Read, Update, Delete) operations.
- Design data integrations required between the Reference Data Management service and reference data source systems (Extract, Transform, Load).
- Develop an ongoing change and testing strategy for the Reference Data Management service.
- Participate in DD CDO led Data Domain working groups for DefSp.
- Identify Reference Data that is Managed and Mastered by Industry Partners and used as Reference Data in DefSp EWSS (Enterprise-Wide Support Services). Work with DD CDO to recommend an appropriate architecture for managing this data.
- Work with DD Data Catalogue & Curation (DCC) team to explore the option of extending the current R360 service to provide a Pan Defence RDM service.
- Support with DD DCC team to design & develop OSM (Operating Service Model) / ITSM (Information Technology Service Management) for the R360 service.
- Engage with other Top-Level Budgets (TLBs) through Data Domain Working groups to resolve conflicts of Reference Data sets.

**OFFICIAL-SENSITIVE COMMERCIAL****Required outputs/deliverables/milestones.**

The partner is required to deliver the following activities within the Business Modernisation for Support Programme during the period November 2024 to April 2025.

The first 4-week phase (DCDR 1 and DCDR 2) in which the partner will analyse the architecture, elicit requirements, and create agreed Minimum Viable Products (MVPs) to test if user expectations can be met.

This work will then support the creation of a plan to implement the remaining objectives, for the subsequent weeks, which will be produced and agreed with MOD stakeholders at the end of the initial phase.

The key phases and activities are summarised under the following main categories:

**DCDR 1: Data Catalogue Analysis & Design, four weeks (from contract award) to:**

- Document and agree the ways of working, execution of workshops and establish communication plans with key partners and consumers of the support data e.g., DD CDO (Chief Data Office), DefSp data stakeholders and other MOD Data teams.
- Document and agree a prioritised list of data sets and attributes to be fully catalogued.
- Document and agree initial use cases, deliverables and timelines based on use case prioritisation.
- Facilitate appropriate workshops and meetings between the domains and communities for SDW data.
- Define the interaction of the Data Catalogue service with the existing operational governance and data stewardship model and recommend changes.
- Elicit Data Catalogue requirements from the key stakeholders and consumers.
- Conduct a gap analysis of the current catalogue architecture and identify any issues that may impact DefSp objectives being achieved.

**OFFICIAL-SENSITIVE COMMERCIAL**

- Estimate and document anticipated metadata volumes within the Data Catalogue service.
- Define roles and responsibilities of DefSp data governance stakeholders including data owners and data stewards related to project execution and produce a RACI matrix.
- Document training needs and frequency of workshops throughout delivery to upskill MOD stakeholders with product features and the art of the possible with the data that has been ingested to the data catalogue.
- Document high-level design (HLD) highlighting the scope for the delivery of the Minimum Viable Product (MVP) delivery.
- Coordinate HLD approval with MOD design authority.
- Create a plan for the population and future maintenance of the DefSp Data Catalogue.

**DCDR 2: RDM Planning and MVP design, four weeks (from Contract Award) to:**

- Review of DefSp Functional Blueprint for Data, and functional/non-functional requirements set for RDM service, facilitation of stakeholder workshops to understand the overall strategic vision & design of how these will be met in R360 (including a review of the EnACT report).
- Document business objectives and the current technical landscape, business challenges, existing reference data sets and data producers/owners.
- Document understanding of As-Is system handling of reference data and the processes involved.
- Discovery of Support Reference Data and creation of an offline catalogue defining internal & externally sourced Reference Data (RD).
- Document data sources for reference data, integration approaches and recommendations and designs for future reference data processing, identifying any issues with managing these into the R360 service.
- Identify and document reference data consumption requirements relating to current/future Support digital services.
- Work with the authority to define an achievable MVP RDM service based on analysis of the candidate reference datasets and BMfS programme dependencies on the service.

**DCDR 3: Data Catalogue Content Creation MVP to:**

- Create and develop catalogue content for in-scope data sets as specified based on the HLD.
- Create the required metadata for prioritised Critical Data Elements in the Data Catalogue, including an example of de-conflicting definitions using the Data Glossary and recording data lineage.
- Document and capture the risks and challenges with data-set ingestion and augmentation.
- Use the catalogue to document the dependency between the SDW and its source/consuming systems.
- As required to deliver the MVP configure Informatica services and connectors as specified in the HLD.
- Define and implement the roles and responsibilities for Data Stewards in relation to future Catalogue management.
- Catalogue the agreed attributes from the SDW so that they are accessible to all users of the catalogue.
- In partnership with the DD CDO, define how new data consumers can find and exploit the catalogue service, focussing on priority use cases.
- Agree a future plan and roadmap, for creating data catalogue entries for all BMfS in-scope applications.

**DCDR 4: RDM setup, configuration and documentation to:**

**OFFICIAL-SENSITIVE COMMERCIAL**

- Set up and configuration of the R360 environments required to deliver the service working with DD CDO team and BMfS testing team.

**OFFICIAL-SENSITIVE COMMERCIAL**

- Delivery/configuration of integration capability required to ingest and publish in scope reference data sets.
- Design and implement role-based access to the service, utilising the authority provided SSO solution.
- Completion of unit testing (or equivalent) for any areas of configuration of R360, such as workflow & integration (must cover any bespoke change made to R360).
- Integration testing for the SSO Solution with the authority.
- Undertake service testing and provide test completion reports to the BMfS Test Lead on completion of test phases covering the spread of testing activity completed.
- Work with CIO/BMfS/DD teams to document key RDM processes and create training material.
- Review of the Target end state delivery model for BMfS and make recommendations for how this will deliver and support the reference data service.
- Creation of on-boarding briefing material relating to the reference data service for BMfS contracted System Integrators.

**DCDR 5: Reference data ingestion and planning of next stage to:**

- Ingestion of priority reference data into the R360 service for identified MVP scope, including testing of data integrity once imported.
- Define required hierarchies within the Reference data for the MVP.
- Develop and implement validation rules for the MVP RD sets if appropriate.
- Resolution of identified bugs or defects conducted by the authority at the agreed test phases, which are related to areas of the service configured or populated with data by the supplier.
- Evaluate the overall effectiveness of R360 functions and features in meeting the scope of the MVP. Provide recommendation for how The Authority can implement R360 to meet the Defence Support future requirements, including analysis of tooling features against the requirements.
- Estimate potential costs of full-scale implementation of R360 based on the MVP delivery experience.
- Validate that the design of the DefSp Reference Data Management service meets the needs of the BMfS programme but that it is also in line with wider DD CDO strategy for reference data management.
- Document the logical and physical architecture of the deployed RDM service including all service/system integrations.

**OFFICIAL-SENSITIVE COMMERCIAL****Proposed charges**

Proposed charges should cover the 6-month delivery of DCDR 1 – DCDR 5. Further deliverables will be identified and costed for the optional extension period.

Payment will be Fixed Price in accordance with the following milestones:

- *DCDR 1 – **Data Catalogue Analysis & Design***
- *DCDR 2 – **RDM Planning and MVP design***
- *DCDR 3 – **Data Catalogue Content Creation MVP***
- *DCDR 4 – **RDM setup, configuration and documentation***
- *DCDR 5 – **Reference data ingestion and planning of next stage.***

Amounts to exclude VAT and Travel and Expenses (T&E).

**Acceptance**

The Supplier will demonstrate the deliverables achieved in the Discovery phase via one or more “show and tell” sessions.

These sessions will showcase the relevant artefacts and business value achieved to named BMfS and Sp CIO representatives (including the DefSp Solution Integration Authority (SIA)).

To support transparency, the named BMfS or Sp CIO representatives can query or comment on any completed work during delivery.

Changes to the agreed statement of work can be requested by a senior MOD representative, which may cause a change in schedule, prioritisation, or pivot of work. These change requests must be agreed upon with the Supplier’s programme leads.

Any changes to the contract will require a contract amendment, as per the contract change process.

**OFFICIAL-SENSITIVE COMMERCIAL**



**OFFICIAL-SENSITIVE COMMERCIAL**

