

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 2 - Dev, Apps, UX, Dev Ops, Sys Design & Support

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

Call-Off Reference	RM6249/DIPS (2) 046	Version Number	1	Date	01/07/24

Business Case Reference	Original FBC Number	22100 Data Cataloguing Curation Enterprise Tooling BusinessCase v003.2.docx (sharepoint.com)		
	Amendment FBC Number	20240606- DCC Commitment Case Jul 24 to Mar 25.docx		
Project / equipment for which Services are in support	PO093 - Data Curation and Cataloguing part of the Data Strategy for Defence SOW5	Urgent Capability Requirement (UCR)	N/A	
Call-Off Contract title:	PS461 Defence Management Service for Data Mgt and Curation Tool			
Call-Off Contract description:	To provide activities to achieve the objective of providing DMGS with a comprehensive tool-based capability to define and catalogue its data assets in the Defence Data Catalogue (DDC). Key to this is providing information on its quality, ownership and the relevant policies required to access and use it across the MOD			
1b. Contact details				

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

Government Directorate / Organisation Title		Name of Supplier	Capgemini UK plc
Name of Requirement Holder's Authorised Representative		Name of Supplier's Authorised Representative	
Post title		Post title	
Requirement Holder's Address	Ground Floor, Zone D MoD Main Building Whitehall London, SW1A 2HB	Supplier Address	1 Forge End Woking GU21 6DB
Postcode		Postcode	
Telephone		Telephone	
Email		Email	
Unit Identification Number (UIN)	D2118A	Value Added Tax (VAT) Code	
Resource Accounting Code (RAC)	6903		
Name of Requirement Holder's Project Lead			
Requirement Holder's Secondary Contact Name		Supplier Secondary Contact Name	

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

Requirement Holder's Secondary Contact Role	<div style="background-color: black; width: 150px; height: 20px;"></div>	Supplier Secondary Contact Role	
Requirement Holder's Secondary Contact Email	<div style="background-color: black; width: 150px; height: 20px;"></div>	Supplier Secondary Contact Email	

Date that the Statement of Requirements was issued	28/06/2024	Deadline for Requirement Holder's receipt of Supplier's Call-Off Tender	N/A
---	------------	--	-----

Background/justification for Call-Off Contract

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

The DMGS team within the Data Programme have work in progress on the Data Cataloguing and Curation programme, this contract continues this work via DIPS Direct Award of a new managed services contract from July 2024 until March 2025. This DIPS Direct Award contract is placed on an exceptional basis to maintain momentum and continuity whilst a full competition is initiated and concluded under the DIPS framework.

1 Statement of Requirements (SOR)

Unique Order Number (defined by delivery team)	PO093		
SOR version issue number	1	SOR dated	28/06/24
SOR title	Data Cataloguing & Curation Programme SOW 5		

Description of Services to be provided under the Call-Off Contract
See Appendix 3 – SOW
Activities required to be undertaken under the Call-Off Contract
See Appendix 3 - SOW
Outputs to be provided under the Call-Off Contract
See Appendix 3 - SOW
Acceptance/rejection criteria / provisions
See Appendix 3 - SOW
Material KPIs / Critical Service Level Failure

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

The following Material KPIs shall apply to this Call-Off Contract in accordance with Framework Schedule 4 (Framework Management):

Material KPIs

Not applicable

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

Not applicable

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

MOD MoDNet Laptops / Virtual Desktop - x1 per staff member

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:

- AQAP 2131 Edition C Version 1 NATO Quality Assurance Requirements for Final Inspection and Test. CoC shall be provided in accordance with DEFCON 627 • 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
- Processes and controls for the avoidance of counterfeit materiel shall be established and applied in accordance with Def Stan. 05-135, Issue 2 – Avoidance of Counterfeit Materiel.

Project and risk management

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

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	15th July 2024
Call-Off Initial Period	8.5 months
Call-Off Expiry Date	31 st March 2025
Call-Off Optional Extension Period	N/A
Minimum notice period prior to a Call-Off Optional Extension Period	N/A

SOR approved by (Name in capital letters)	<div></div>	Telephone	<div></div>
Directorate / Division	<div></div>	Email	<div></div>

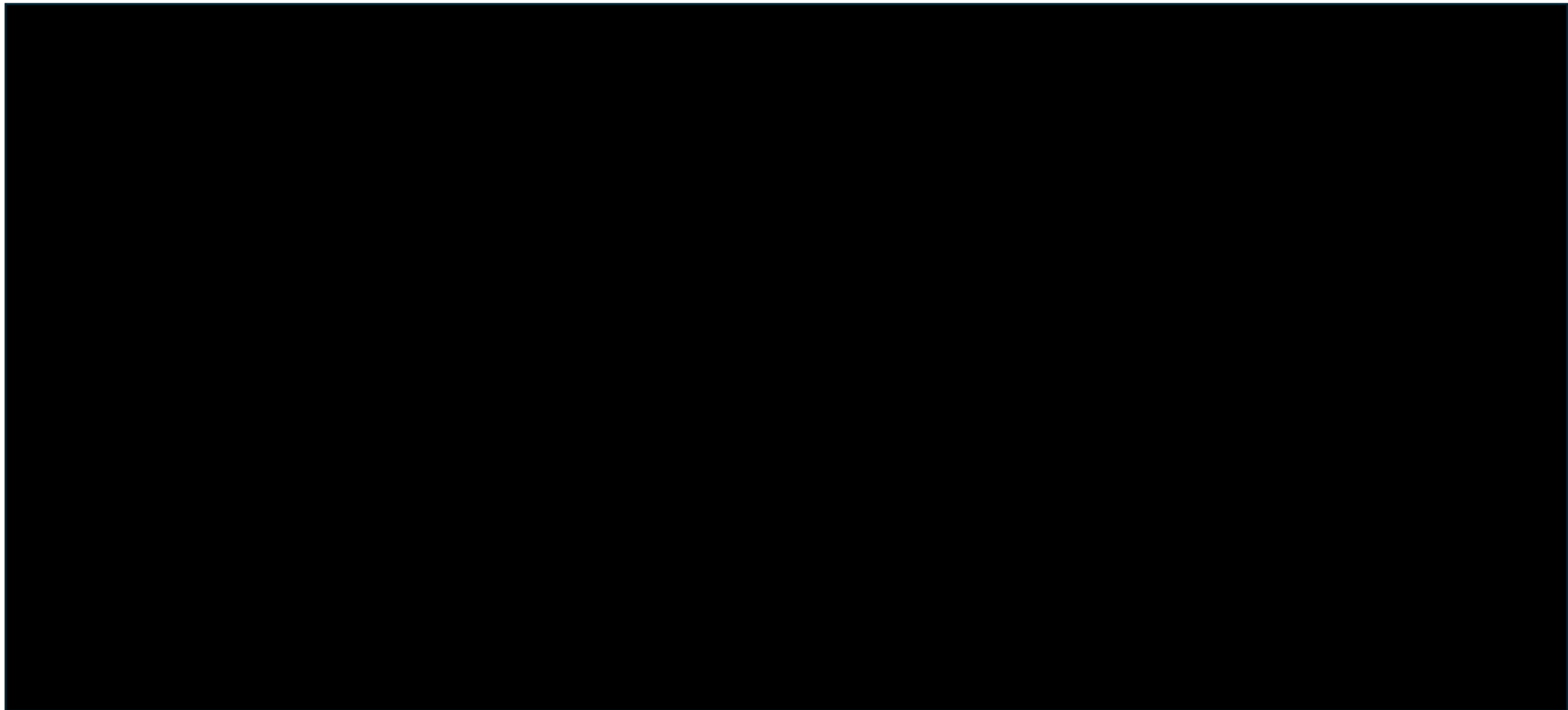
Organisation Role / Position	<div></div>	Date	
------------------------------	-------------	------	--

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

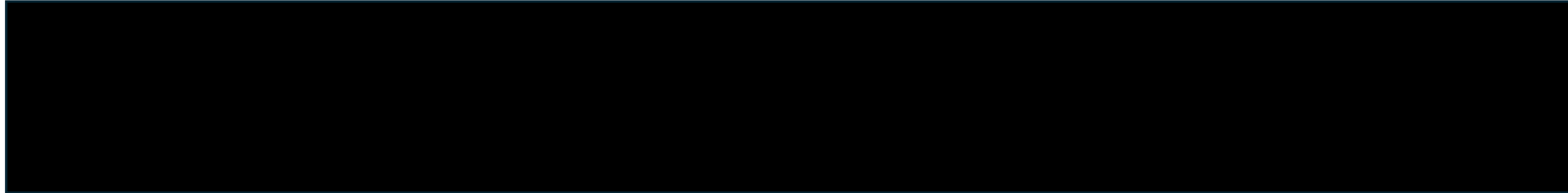
Approver's signature	
----------------------	--

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

Original FBC Number (when known)	Amendment FBC Number (if applicable)
See section 1a	See section 1a

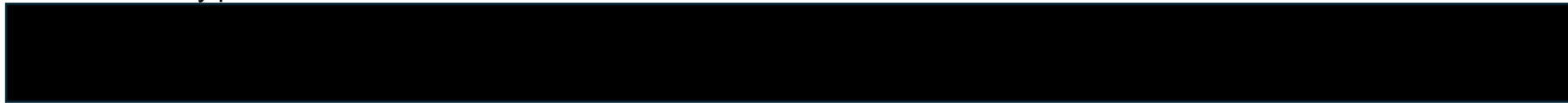


DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)



Delivery Plan:

The draft delivery plan below illustrates the activities and deliverables for the duration of the SoW:



The actual delivery timescales may vary and are dependent on the Buyer dependencies and obligations.

Acceptance of Deliverables:

The Supplier will provide the Buyer with a Monthly Progress Report (to be issued in the week before the end of the month), which will contain details of all deliverables completed within the applicable month. The Supplier and Buyer will hold an Assurance Meeting, within one week of issuing the Monthly Progress Report to review and confirm that the deliverables satisfy the acceptance criteria and deliverable descriptions in Table 1 – Deliverables. Following the Assurance Meeting the Buyer will provide either:

- i) acceptance in writing of the deliverables within 5 working days or
- ii) if a deliverable is not accepted, the Buyer will provide feedback on where the Deliverables do not meet their descriptions, followed by written feedback, and the Supplier will remediate the deliverable for subsequent review/approval by the Buyer.

The Supplier will only submit an invoice for a payment when ALL Deliverables corresponding to the applicable payment milestone as set out in the Milestone Payment Schedule below have been accepted by the Buyer in accordance with the above process. No invoices shall be submitted by the Supplier or payments made by the Buyer for progress made towards completion of deliverables.

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

Dependencies:

Ref	Dependencies and Obligations of the Buyer	Required by Date	Deliverables which cannot be delivered if dependency is not met	Deliverables where timely and effective delivery will be impacted if dependency is not met
DEP-01	Buyer will ensure reasonable, timely access to relevant MOD people, resources and documentation required for the delivery of the services, subject to the supplier providing adequate prior notice. (For example, access to key stakeholders for the candidate systems to be catalogued e.g. SDW, MyHR, CP&F, DE&S AE and ADW)	Ongoing		All SOW deliverables
DEP-02	Buyer will ensure that the Supplier has the necessary access rights, permissions and uninterrupted access to any MOD systems and data required for delivery of the services, subject to reasonable prior notice and the supplier staff having the required security clearance.	Ongoing		All SOW deliverables
	Buyer will procure, provide and maintain for the duration of the SOW the licenses for the software for such MOD systems to be used.			

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

DEP-03	Buyer will provide Supplier resources with MODnet accounts, virtual desktops and MOD laptops , within 2 weeks of joining the DC&C Programme, subject to the supplier complying with the appropriate buyer onboarding process. This will enable access to MODnet Intranet, SharePoint sites, DAR, RDM, DaVinci, and to the Digital Foundry Agile Toolset	Ongoing		All SOW deliverables
DEP-04	Buyer will ensure that Data Stewards will be appointed by data domain and available to engage with the DC&C Programme.		D09, D21, D22, D24, D25	

Table 2 – Dependencies and Obligations of the Buyer

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]
- 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 7 (Financial Difficulties) **Not required** ○ Joint Schedule 8 (Guarantee) **Not required** ○ Joint Schedule 10 (Rectification Plan) ○ Joint Schedule 11 (Processing Data)
 - Call-Off Schedules
 - Call-Off Schedule 2 (Staff Transfer), Part D ○ 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 8 (Business Continuity and Disaster Recovery) ○ Call-Off Schedule 9 (Security) – Part A
 - Call-Off Schedule 10 (Exit Management) ○ Call-Off Schedule 17 (MOD Terms) ○ Call-Off Schedule 25 (Ethical Walls Agreement) ○ 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.

2a. Strategy for procurement and evaluation

DIPS Order Form / Statement of Requirements Template

(Framework Schedule 6)

Further competition	<input type="checkbox"/>				
Direct award	<div style="color: blue; font-weight: bold;">XError!</div> <div style="color: blue; font-weight: bold;">Bookmark not defined.</div>	Competitive award criteria to be used for undertaking evaluation of proposal(s)	Direct award		
		Weighting (Technical)	N/A	Weighting (Price)	N/A

2b. General Conditions

Additional general DEFCON/conditions and DEFFORMs applicable to providing the Deliverables, are to be listed here:

Additional Conditions: Deform 94 Confidentiality Agreement (Appendix 5 for individuals)

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.



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"/>
Incremental Fixed Price	<input type="checkbox"/>
Time and Materials (T&M)	<input type="checkbox"/>
Fixed Price	X <input checked="" type="checkbox"/>
A combination of two or more of the above Charging methods	<input type="checkbox"/>
T&S is applicable	<input type="checkbox"/>
No T&S is available	

2e. Payment Method

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

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 18th August 2023.

2i. Requirement Holder's Security Policy

Security Aspects Letter to be issued and executed alongside this Order Form. See Appendix 6.

2j. Progress Reports and meetings

Progress Report Frequency	Monthly	Progress Meeting Frequency	Monthly
---------------------------	---------	----------------------------	---------

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.	<input type="checkbox"/>
--	--------------------------

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

Deliverable Quality Plan requirements:

DEFCON 602A (<i>Edn 12/17</i>) - Quality Assurance with Quality Plan	<input type="checkbox"/>	DEFCON 602B (<i>Edn 12/06</i>) - Quality Assurance without Quality Plan	X
--	--------------------------	---	---

AQAP 2105:2 – NATO Requirements for Deliverable Quality Plans	<input type="checkbox"/>
---	--------------------------

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	<input type="checkbox"/>
--	--------------------------

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)	OBJ: <input type="checkbox"/>
Relevant MAA Regulatory Publications (See attachment for details)	OBJ: <input type="checkbox"/>
Additional Quality Requirements (See attachment for details)	OBJ: <input type="checkbox"/>
Planned maintenance schedule requirement	
N/A	OBJ: <input type="checkbox"/>

2l. Key Staff

OFFICIAL SENSITIVE (when complete)

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

Not applicable

2m. Key Subcontractor(s)

Not applicable

2n. Commercially Sensitive Information

1. Details of the Supplier's methodologies, policies and processes
2. All information relating to limits of liability, daily fee rates, pricing and charging mechanisms contained in the Call-Off Contract
3. The terms of the Supplier's insurance
4. All details relating to personnel including but not limited to the numbers of resources with specific skills, numbers of security cleared staff, staff terms and conditions of employment and staff selection methods
5. Any information relating to other customers of the Supplier

2o. Cyber Essentials

Cyber Essentials Scheme: 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).

Risk
Assessment
Ref:
240605A13
Cyber Risk
profile:
N/A **Error !
Bookmark
not**

OFFICIAL SENSITIVE (when complete)

defined.

2p. Implementation Plan

Implementation Plan requirements in accordance with paragraph 1.1 of Call-Off Schedule 13 (Implementation Plan).]



3. Charges

Estimated Contract Value (excluding VAT) for Call-Off Contract

£2,499,108 excl VAT as detailed in section 2f

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)

Not applicable

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		Email	
Organisation Role / Position		Date	11 Jul 2024
Approver's signature			

8. Acknowledgement by Supplier

Order Form acknowledged by (Name in capital letters)		Telephone	
Supplier Name		Email	
Supplier Role / Position		Date	
Approver's signature			

9. Final Administration

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

Appendix 1 - Addresses and Other Information

1. Commercial Officer Name:

Address: [Defence Digital | Strategic Command | Commercial Spur B2, Building 405, Westwells Road, MoD Corsham, Wiltshire, SN13 9NR](#)

Email:

8. Public Accounting Authority

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

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

Name:

Address

[Ground Floor, Zone D | MoD Main Building | Whitehall | London, SW1A 2HB](#)

Email:



3. Packaging Design Authority Organisation & point of contact:

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



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



(b) U.I.N.

9. Consignment Instructions

The items are to be consigned as follows:

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

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

[Air Freight Centre](#)

IMPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943

EXPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943

[Surface Freight Centre](#)

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

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

B. JSCS

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

JSCS Fax No. 01869 256837

Users requiring an account to use the MOD Freight Collection Service should contact [UKStratCom-DefSpRAMP@mod.gov.uk](#) in the first instance.

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

5. Drawings/Specifications are available from

11. The Invoice Paying Authority

Ministry of Defence ☎ 0151-242-2000
DBS Finance
Walker House, Exchange Flags Fax: 0151-242-2809
Liverpool, L2 3YL **Website is:**
<https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement>

6. Intentionally Blank

12. Forms and Documentation are available through *:

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

Leidos-FormsPublications@teamleidos.mod.uk

7. Quality Assurance Representative:

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

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

*** NOTE**

1. Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Internet Site:
<https://www.kid.mod.uk/maincontent/business/commercial/dex.htm>
2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.

Appendix 2 – Supplier's Quotation - Charges Summary

Supplier Charges summary: To be completed by the Supplier in support of a quotation provided in response to an ITT for the requirement captured on the above Order Form.

1. To: [REDACTED]
Head of Data Management, Governance and Skills
Development
Ground Floor, Zone D | MoD Main Building | Whitehall |
London, SW1A 2HB

2. From: [REDACTED]

Date of tender submission:

In response to the Order Form request for a quotation Dated reference

*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:

10/07/2024

2. Call-Off title: PS461 Defence Management Service for Data Mgt and Curation Tool

3. Supplier Unique Reference Number: PO093

4. Start Date: 15 July 2024 Completion Date: 31 March 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 (£) (excl. VAT)
------------------------------	-------	--------------------------	---------------------------------	--------------------------------	------------	-----------------------



Total			2,499,108

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)	0)
	Air))
	Sea))
	(Estimated expenditure on:)	Unit cost	Number of Night / Days	Total
5c. Subsistence	Accommodation (max £100 per night incl VAT)	0	0	0
	Meals (max £5 for lunch and/or £22.50 for an evening meal, including all drinks)	0	0	0
	Miscellaneous costs (please define below)	0	0	0
	The above T&S costs relate to the period to			
<u>Subcontractor price</u>				
5d. Other Costs	Subcontractor Details 0			
	Materials 0			

Other		
(Please provide details below)		
Description		Cost
0		0
Total Charges for completion of Call-Off Contract Deliverables		£2,499,108..... (excl. VAT)

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:

SOW Title: Defence Data Catalogue Programme SOW 5

SOW Reference: Defence Data Catalogue Programme SOW 5 T-045

Call-Off Contract Reference: PS461 Digital & IT Professional Services (DIPS)

Requirement Holder: [REDACTED]

Supplier: Capgemini UK plc

SOW Start Date: 15/07/24

SOW End Date: 31/03/25

Duration of SOW: 8.5 months

Key Personnel (Requirement Holder): [REDACTED]

Key Personnel (Supplier):

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.

Subcontractors: None

2. Call-Off Contract Specification – Deliverables Context

SOW Deliverables Background:

The Data Cataloguing and Curation (DC&C) Programme (the 'Programme') is part of the Data Strategy for Defence and Data Transformation programme to underpin the realisation of "Data as a Strategic Asset" for Defence.

Interoperable, governed, and curated data will be delivered through embedding the Defence Data Governance Framework across Defence and the completion of the Defence Data Catalogue (DDC) which will provide a searchable index for Defence metadata, making it discoverable, traceable, and available for exploitation.

The DC&C Programme focuses on metadata assets across the MOD's 15 Data Domains to:

- Promote a cross-Defence data catalogue capability.
- Provide a means for achieving cross-Defence agreement on, for example: critical data elements (CDEs), business glossary, data quality rules and data hierarchies.

Populating the DDC with relevant metadata is achieved by:

- Establishing and running Metadata Forums to: develop and curate a Business Glossary of business term definitions; curate technical metadata; and develop data quality rules, data hierarchies and data policies.
- Cataloguing prioritised MOD source IT systems and scanning and harvesting relevant technical metadata.
- Ingesting data products to provision through the Data Marketplace.

Once populated, the DDC provides the capability for Business and IT teams across TLBs and the 15 Data Domains to curate assets and exploit the metadata content, including using the Data Marketplace. Rollout and adoption of the DDC across Defence will be via a 'franchise model', enabling Business and IT teams to prioritise content and provision a selfserve data exploitation capability.

Delivery Streams:

The DC&C Programme will deliver the DDC via 4 delivery streams:

1. **Stakeholder Engagement:** The Programme will focus on raising awareness of the benefits of the DDC across Defence and promoting exploitation of the DDC in critical Defence transformation programmes, in particular DDAP, Data Fabric, CSM, BMfS and DX4D. A prioritised list of key MOD IT systems to be catalogued will be developed, together with TLB/Domain agreement on providing the necessary resources to support the cataloguing process.
2. **Catalogue Population** – This stream has four components:
 - a. **Metadata Forums (MDFs).** The Programme establishes and runs the MDFs with the individual domain and sub-domain SMEs. Each Domain also provides one or several 'Data Steward(s)' and the DC&C team transition the running of the MDFs to the Data Stewards, allowing the programme team to engage new Domains.
 - b. **Systems Cataloguing.** The Programme develops the means/connections to catalogue the systems, prioritised by Demand Management, which are in turn aligned to Domains with the MDFs. This stream is heavily dependent on Digital Foundry providing key MOD IT system connection services.
 - c. **Catalogue Factory.** The Programme uploads the developed business metadata assets into the DDC. In parallel, it runs scans on the prioritised systems and harvests relevant technical metadata into the DDC.
 - d. **Catalogue Capability.** The Programme investigates additional capability around DataCards to support Defence Artificial Intelligence Centre (DAIC), and Informatica CDAM feature-set to be used in Data Marketplace provisioning.

3. **Rollout & Adoption** – The Programme will design and implement a ‘franchise approach’ for the rollout of the DDC, which will enable TLBs/Domains to connect to the DDC and catalogue and curate their data assets on a self-serve basis.
4. **Programme Governance** – Implementation of the DDC will be managed and reported against defined KPIs in Monthly Progress Reports and be reviewed at regular DC&C Programme Boards.

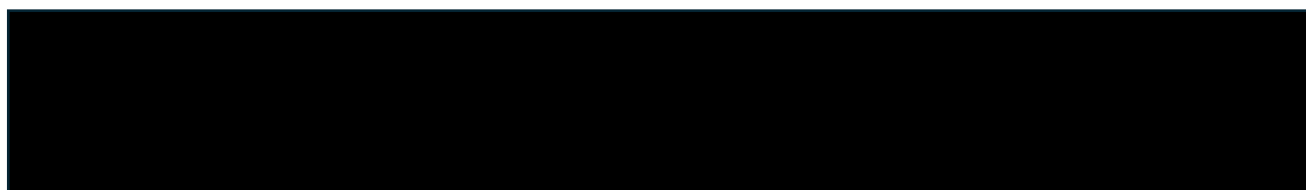
Overview of Requirement:

3. Requirement Holder Requirements – SOW Deliverables

Outcome Description:

The following table provides details of each Deliverable that the Supplier shall deliver to the Buyer, subject to the Buyer meeting the Dependencies stated in this SOW. Detailed ‘deliverable descriptions are also provided at Annex 1.

Table 1 – Deliverables

A large black rectangular box redacting the content of Table 1.

*Detailed ‘Deliverable Descriptions’ and Acceptance Criteria are provided at Annex 1 **
The Deliverable Due Dates are dependent on the Buyer dependencies set out in Table 2 below.

Delivery Plan:

The draft delivery plan below illustrates the activities and deliverables for the duration of the SoW:

The actual delivery timescales may vary and are dependent on the Buyer dependencies and obligations.

Acceptance of Deliverables:

The Supplier will provide the Buyer with a Monthly Progress Report (to be issued in the week before the end of the month), which will contain details of all deliverables completed within the applicable month. The Supplier and Buyer will hold an Assurance Meeting, within one week of issuing the Monthly Progress Report to review and confirm that the deliverables satisfy the acceptance criteria and deliverable descriptions in Table 1 – Deliverables.

Following the Assurance Meeting the Buyer will provide either:

OFFICIAL SENSITIVE (when complete)

- i) acceptance in writing of the deliverables within 5 working days or
- ii) if a deliverable is not accepted, the Buyer will provide feedback on where the Deliverables do not meet their descriptions, followed by written feedback, and the Supplier will remediate the deliverable for subsequent review/approval by the Buyer.

The Supplier will only submit an invoice for a payment when ALL Deliverables corresponding to the applicable payment milestone as set out in the Milestone Payment Schedule below have been accepted by the Buyer in accordance with the above process. No invoices shall be submitted by the Supplier or payments made by the Buyer for progress made towards completion of deliverables.

Dependencies:

Table 2 – Dependencies and Obligations of the Buyer

Ref	Dependencies and Obligations of the Buyer	Required by Date	Deliverables which cannot be delivered if dependency is not met	Deliverables where timely and effective delivery will be impacted if dependency is not met
DEP-01	Buyer will ensure reasonable, timely access to relevant MOD people, resources and documentation required for the delivery of the services, subject to the supplier providing adequate prior notice. (For example, access to key stakeholders for the candidate systems to be catalogued e.g. SDW, MyHR, CP&F, DE&S AE and ADW)	Ongoing		All SOW deliverables

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

DEP-02	Buyer will ensure that the Supplier has the necessary access rights, permissions and uninterrupted access to any MOD systems and data required for delivery of the services, subject to reasonable prior notice and the supplier staff having the required security clearance. Buyer will procure, provide and maintain for the duration of the SOW the licenses for the software for such MOD systems to be used.	Ongoing		All SOW deliverables
DEP-03	Buyer will provide Supplier resources with MODnet accounts, virtual desktops and MOD laptops , within 2 weeks of joining the DC&C Programme, subject to the supplier complying with the appropriate buyer onboarding process. This will enable access to MODnet Intranet, SharePoint sites, DAR, RDM, DaVinci, and to the Digital Foundry Agile Toolset	Ongoing		All SOW deliverables
DEP-04	Buyer will ensure that Data Stewards will be appointed by data domain and available to engage with the DC&C Programme.		D09, D21, D22, D24, D25	

Supplier Resource Plan:

There is no Supplier Resource Plan associated with this SOW.

The Supplier resources will be based at resources' home locations or the below Supplier or Buyer office locations:

- Ministry of Defence, Main Building, Whitehall Horse Guards Avenue, London, SW1A 2HB.
- Capgemini UK plc, 40 Holborn Viaduct, Holborn, London, EC1N 2PB.

Security Applicable to SOW:

The Supplier confirms that all Supplier Staff working on Requirement Holder Sites and on Requirement Holder Systems (as defined in Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) and Deliverables, have completed Supplier Staff vetting in accordance with any applicable requirements in the Contract, including Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security).

Call-Off Schedule 9 (Security) – Part A applies to this SoW.

SOW Standards:

- No specific Quality Management System requirements are defined. This does not relieve the Supplier of providing conforming products under this contract. CoC shall be provided in accordance with DEFCON 627
- 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

Performance Management:

Reporting and management of performance against submission/acceptance of deliverables against plan.

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:

Not applicable

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:

- A Weekly Status Report
- A Monthly Progress Report

4. Charges

Call Off Contract Charges:

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

- Fixed Price

The value of this SOW (irrespective of the selected charging method) is
£ 2,499,108 (excl VAT). £ 2,998,929. (inc VAT)

Milestone Payments Schedule:

The Milestone Payments Schedule is detailed below in Table 4 – Milestone Payments Schedule. The Buyer will pay the Supplier, following satisfactory delivery and final acceptance of the monthly deliverables, as per Table 4 – Milestone Payments Schedule.

Table 4 – Milestone Payments Schedule – all values in £ GBP

A large black rectangular box redacting the content of Table 4, which would detail the Milestone Payments Schedule.

Rate Cards Applicable:

Not applicable.

Reimbursable Expenses:

[See Expenses Policy in Annex 1 to Call-Off Schedule 5 (Pricing Details and Expenses Policy)] The Buyer will pay for Supplier travel expenses where the Supplier is required to be on site at a location that is not Main Building, London, subject to such expenses being agreed prior to them being incurred.

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: [REDACTED]

Date: 10/07/2024

Signature: [REDACTED]

For and on behalf of the Requirement Holder

Name: [REDACTED]

Title: Dep Hd, Prof Svcs, Defence Digital Commercial

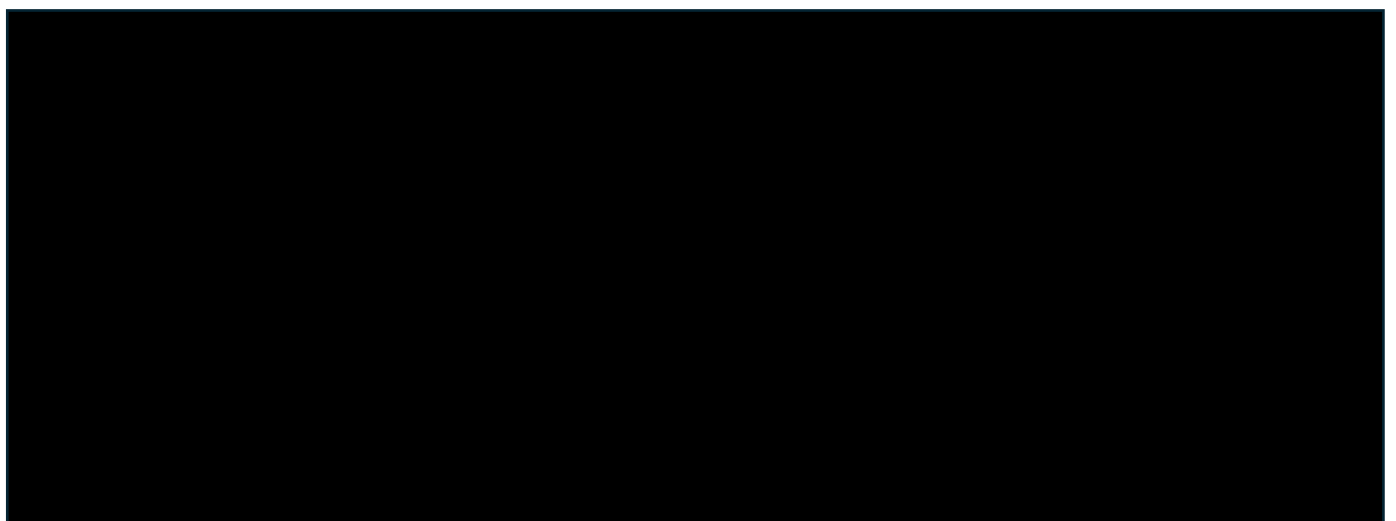
Date: 11 July 2024

Signature: [REDACTED]

Annex 1 to Statement of Work

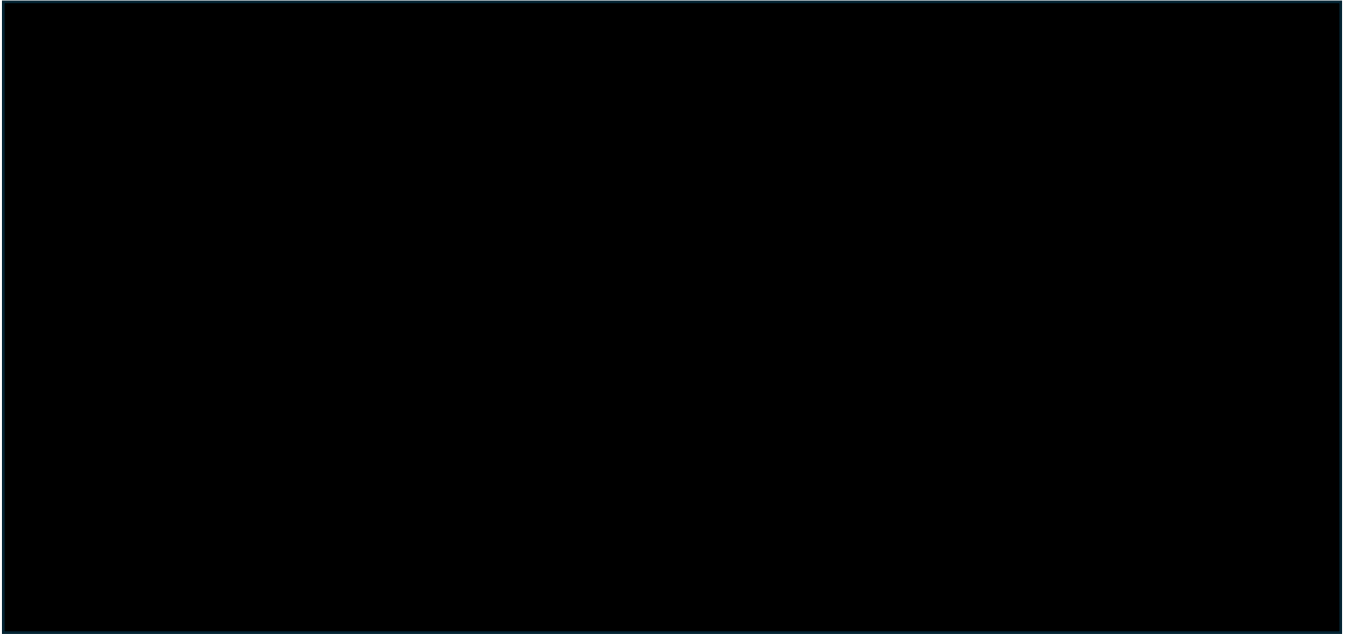
Deliverable Descriptions

Stakeholder Engagement

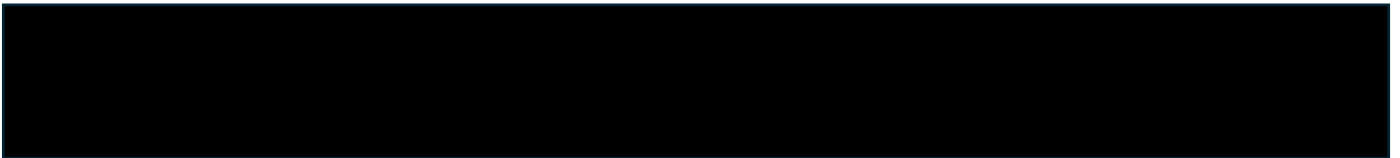


Catalogue Population – Metadata Forums

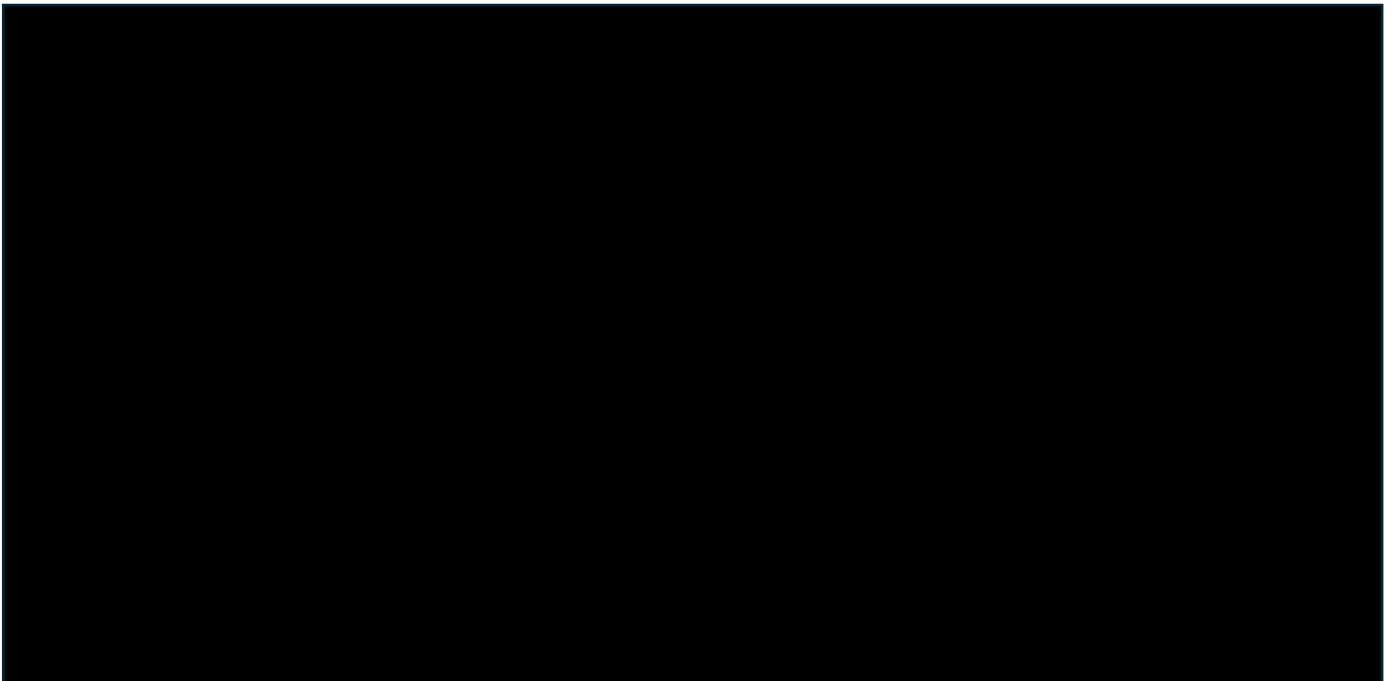
Catalogue Population – Systems Cataloguing



Catalogue Population – Catalogue Capability



Rollout and Adoption



Programme Governance



Annex 2 to Statement of Work

Data Processing

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>The Parties are Independent Controllers of Personal Data</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p>Business contact details of Supplier Personnel for which the Supplier is the Controller,</p> <p>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 the Relevant Authority is the Controller,</p> <p>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</p>
	<p>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.</p>
Duration of the Processing	15 th July 2024 to 31 st March 2025
Nature and purposes of the Processing	<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: Data processing and curation, working along side civil servants for knowledge transfer.</p>
Type of Personal Data	Name, address, date of birth, telephone number, email address, work location and details, home address.

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

Categories of Data Subject	Personnel (including volunteers, agents, and temporary workers), customers / clients, suppliers.
----------------------------	--

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 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

OFFICIAL SENSITIVE (when complete)

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

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 6 Security Aspects Letter

Secretary of State for Defence, acting by the Directorate of the UK Strategic Command,

Defence Digital, Building 405, MOD Corsham, Westwells Road, Corsham, Wiltshire, SN13 9NR

Date of Issue: 02/07/2024

For the attention of:



Capgemini UK plc
1 Forge End
Woking
GU21 6DB

ITT/CONTRACT NUMBER & TITLE: PS461 - Defence Management Service for Data Mgt and Curation Tool SOW5

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 [See Annex B] outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.
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 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.]

OFFICIAL SENSITIVE (when complete)

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

- 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 coordination 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](#)

ANNEX C: 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: SPODSR-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 and UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading.

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 register the IT system onto the Defence Assurance Risk Tool (DART). Details on the registration process can be found in the 'Industry Security Notices (ISN)' on Gov.UK website. ISNs 2017/01, 04 and 06, Defence Condition 658 and Defence Standard 05-138 details the DART registration, IT security accreditation processes, risk assessment/management and Cyber security requirements which can be found in the following links:

<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 OFFICIAL and UK OFFICIAL-SENSITIVE material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be subject to a level of control.

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

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

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

Hard Copy Distribution

15. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed, both within and outside Contractor premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

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

Electronic Communication and Telephony and Facsimile Services

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

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

Details of the CPA scheme are available at:

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

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

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 and only with the prior approval of the Authority.

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

Use of Information Systems

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

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

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

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

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

- a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “*least privilege*” will be applied to System Administrators. Users of the IT System (Administrators) should not conduct ‘standard’ User functions using their privileged accounts.
- b. Identification and Authentication (ID&A). All systems are to have the following functionality:
 - (1). Up-to-date lists of authorised users.
 - (2). Positive identification of all users at the start of each processing session.
- c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be “*strong*” using an appropriate method to achieve this, e.g. including numeric and “*special*” characters (if permitted by the system) as well as alphabetic characters.
- d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.
- e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 16 above.
- f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.
 - (1). The following events shall always be recorded:
 - (a) All log on attempts whether successful or failed,
 - (b) Log off (including time out where applicable),
 - (c) The creation, deletion or alteration of access rights and privileges, (d) The creation, deletion or alteration of passwords.
 - (2). For each of the events listed above, the following information is to be recorded:
 - (a) Type of event,
 - (b) User ID,
 - (c) Date & Time, (d) Device ID.

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

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

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

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

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

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

Laptops

25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 16 above.

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites^[1]. 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

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

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 OFFICIAL or OFFICIAL-SENSITIVE material to the Authority. In addition any loss or otherwise compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) below. This will assist the JSyCC 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 WARP will also advise the Contractor what further action is required to be undertaken.

JSyCC WARP Contact Details

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

RLI Email: defencewarp@modnet.rli.uk (MULTIUSER)

Telephone (Office hours): +44 (0) 30 6770 2185 **JSyCC Out of hours Duty Officer:** +44 (0) 7768 558863

Mail: JSyCC Defence Industry WARP X007

Bazalgette Pavilion,

RAF Wyton, HUNTINGDON, Cambridgeshire, PE28 2EA.

30. Reporting instructions for any security incidents involving MOD classified material can be found in Industry Security Notice 2017/03 as may be subsequently updated at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03 - Reporting of Security Incidents.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf)

Sub-Contracts

31. Where the Contractor wishes to sub-contract any elements of a Contract to subContractors 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.

32. The prior approval of the Authority shall be obtained should the Contractor wish to subcontract any UK OFFICIAL-SENSITIVE elements of the Contract to a sub-Contractor facility located in another (third party) country. The first page of Appendix 5 (MOD Form 1686 (F1686) of the GovS 007 Security Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

[https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018 May Contractual process.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf)

33. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 30 above to the sub-Contractor. Contractors located overseas may

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

seek further advice and/or assistance from the Authority with regards the completion of F1686.

Publicity Material

34. 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

Physical Destruction

35. 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 information/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 information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

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

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

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

Audit

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

^[1] Secure Sites are defined as either Government premises or a secured office on the contractor premises.