DEFFORM 8
(Edn 02/24)

Ministry of Defence

Redacted Under FOIA Section 40, Personal Information
Senior Commercial Officer

Kentigern House
65 Brown Street,
Glasgow G2 8EX

Tel:
Redacted Under FOIA Section 40, Personal Information

Redacted Under FOIA Section 40, Personal Information

Your Reference:
710422450
Our Reference:

Date: 01 May 2024

Dear Redacted Under FOIA Section 40, Personal Information
,

Offer Of Call-Off Contract 710422450 for the Provision of Automation Garage (AG) Analysis, Innovation and Development to DBS under DIPS framework RM6249 lot 2

1. As you are aware, the Authority intends to enter into the above call-off contract with you.

2. Please sign and return the enclosed final version of the Framework Schedule 6 (Order Form Template and Call-off schedule) within 5 working days or earlier of the date of this letter to acknowledge your acceptance of the Terms and Conditions.

3. Please note that no Call-Off Contract will come into force until both parties have signed it. The Authority will countersign the Call-off Contract and return a copy of the same to you.

4. The Authority may publish notification of the Call-Off Contract and shall publish Contract documents under the FOI Act except where publishing such information would hinder law enforcement; would otherwise be contrary to the public interest; would prejudice the legitimate commercial interest of any person or might prejudice fair competition in the supply chain.

5. If you wish to make a similar announcement you must seek approval from the named Commercial Officer.

6. Under no circumstances should you confirm to any third party that you are entering into a legally binding call-off contract for Provision of Automation Garage (AG) Analysis, Innovation and Development to DBS prior to both parties signing the Terms and Conditions, or ahead of the Authority's announcement of the Contract award.

Yours sincerely,

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				
Call-Off Reference	RM6249/DIPS(2) 007	Version Number	0	Date	16/02/2024
Business Case Reference	Original FBC Number	DBS/DIT/ITMS/2023/733-093 – Dated 19/12/23			
	Amendment FBC Number	N/A			
Project / equipment for which Services are in support	DBS	Urgent Capability Requirement (UCR)			
Call-Off Contract title:	Automation Garage (AG) Analysis, Innovation and Development				
Call-Off Contract description:	Automation Garage (AG) Analysis, Innovation and Development to support DBS				

1b. Contact details			
Government Directorate / Organisation Title	Defence Business Services	Name of Supplier	Redacted Under FOIA Section 40, Personal Information
Name of Requirement Holder's Authorised Representative	Redacted Under FOIA Section 40, Personal Information	Name of Supplier's Authorised Representative	Redacted Under FOIA Section 40, Personal Information

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

Post title	DBS DIT-AG Service Owner	Post title	*Defence Account Manager*
Requirement Holder's Address	DBS DIT Automation Garage, Oak, East 1, Abbeywood North, Bristol, BS34 8QW	Supplier Address	Redacted Under FOIA Section 40, Personal Information
Postcode		Postcode	
Telephone	Redacted Under FOIA Section 40, Personal Information	Telephone	Redacted Under FOIA Section 40, Personal Information
Email	Redacted Under FOIA Section 40, Personal Information	Email	Redacted Under FOIA Section 40, Personal Information
Unit Identification Number (UIN)	D1041A	Value Added Tax (VAT) Code	*GB232441107*
Resource Accounting Code (RAC)	NPB010		
Name of Requirement Holder's Project Lead	Redacted Under FOIA Section 40, Personal Information		
Requirement Holder's Secondary Contact Name		Supplier Secondary Contact Name	
Requirement Holder's Secondary Contact Role		Supplier Secondary Contact Role	
Requirement Holder's Secondary Contact Email		Supplier Secondary Contact Email	

Date that the Statement of Requirements was issued	16/2/2024	**Deadline for Requirement Holder's receipt of Supplier's Call-Off Tender**	04/03/204

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)	2023/733-093		
SOR version issue number	1.0	SOR dated	16/02/2024
SOR title	DEFENCE BUSINESS SERVICES AUTOMATION GARAGE – ANALYSIS, INNOVATION AND DEVELOPMENT		

Background/justification for Call-Off Contract
Please see Appendix 7
Description of Services to be provided under the Call-Off Contract
Please see Appendix 7
Activities required to be undertaken under the Call-Off Contract
Please see Appendix 7
Outputs to be provided under the Call-Off Contract
Please see Appendix 7
Acceptance/rejection criteria / provisions

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

Please see Appendix 7
Material KPIs / Critical Service Level Failure
Please see Appendix 7
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
Please see Appendix 7
Additional quality requirements & standards (in addition to any quality requirements & standards detailed in the addition to the Call-off Schedules)
Please see Appendix 7
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	09/05/2024 or from contract effective date
Call-Off Initial Period	24 months
Call-Off Expiry Date	08/05/2026
Call-Off Optional Extension Period	12 months
Minimum notice period prior to a Call-Off Optional Extension Period	1 month

SOR approved by (Name in capital letters)	Redacted Under FOIA Section 40, Personal Information	Telephone	Redacted Under FOIA Section 40, Personal Information
Directorate / Division	Defence Business Services	Email	Redacted Under FOIA Section 40, Personal Information
Organisation Role / Position	DBS SIT-AG Service Owner	Date	15/2/2024
Approver's signature	Redacted Under FOIA Section 40, Personal Information		

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

Original FBC Number (*when known*)	**Amendment FBC Number** (*if applicable*)
DBS/DIT/ITMS/2023/733-093 – Dated 19/12/23	N/A

1d. Key Deliverables Template

Statements of Works will be commissioned and agreed through the Contract Period.

Task Number	**Activities to be undertaken and completed by the Supplier**	**Key Deliverables**	**Required Delivery Date**	**List all Requirement Holder Assets issued to Supplier** *(if required)*	**Acceptance Criteria**	**Price £ (Ex VAT)**

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)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data) – replaced by DEFCON 532B (Edn. 12/22) - Protection Of Personal Data (Where Personal Data is being processed on behalf of the Authority) and DEFFORM 532 in appendix 8.

- 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	☒	Competitive award criteria to be used for undertaking evaluation of proposal(s)	Weighted Value for Money Index		
Direct award	☐				
Additional Instructions for completing the Attachment 4 DIPS FC Pricing Response Template: For evaluation purposes only, the Authority has estimated a scenario in number of days per Resource. Once on contract, the Authority reserves the right to commission packages of work or not.		Weighting (Technical)	60%	Weighting (Price)	40%

2b. General Conditions

The Buyer hereby agrees that the requirements of clause 7.4 of the DIPS framework to provide full details of birthplace and parentage are met in full by the security clearance records held by the Ministry of Defence and accessible by the Buyer	☐X

2c. Call-Off Special Terms

The following Special Terms are incorporated into this Call-Off Contract:

DEFCON 076 Edition 11/22 - Contractor's Personnel at Government Establishments
DEFCON 501 (Edn 10/21) - Definitions and Interpretations
DEFCON 503 (Edn 06/22) - Formal Amendments To Contract
DEFCON 513 (Edn 04/22) - Value Added Tax
DEFCON 514 (Edn 08/15) - Material Breach
DEFCON 515 (Edn 06/21) - Bankruptcy and Insolvency
DEFCON 516 (Edn 04/12) - Equality
DEFCON 518 (Edn 02/17) - Transfer
DEFCON 520 (10/23) - Corrupt Gifts and Payments of Commission
DEFCON 522 (Edn 11/21) - Payment and Recovery of Sums Due
DEFCON 524A (Edn. 12/22) - Counterfeit Materiel
DEFCON 526 (Edn 08/02) - Notices
DEFCON 527 (Edn 09/97) - Waiver
DEFCON 529 (EDN 09/97) - Law (English)
DEFCON 530 (Edn 12/14) - Dispute Resolution (English Law)
DEFCON 531 (Edn 09/21) - Disclosure of Information
DEFCON 532B (Edn. 12/22) - Protection Of Personal Data (Where Personal Data is being processed on behalf of the Authority)
DEFCON 534 (Edn 06/21) - Subcontracting and Prompt Payment
DEFCON 537 (Edn 12/21) - Rights of Third Parties
DEFCON 538 (Edn 06/02) - Severability
DEFCON 539 (Edn 01/22) - Transparency
DEFCON 550 (Edn 02/14) - Child Labour and Employment Law
DEFCON 566 (Edn 10/20) - Change of Control of Contractor
DEFCON 602B (Edn 12/06) - Quality Assurance (without Deliverable Quality Plan)
DEFCON 608 (Edn 07/21) - Access and Facilities to be Provided by the Contractor
DEFCON 609 (Edn 07/21) - Contractor's Records
DEFCON 611 (Edn 12/22) - Issued Property
DEFCON 620 (Edn 06/22) - Contract Change Control Procedure
DEFCON 632 (11/21) - Third Party Intellectual Property - Rights and Restrictions
DEFCON 647 (Edn 05/21) - Financial Management Information
DEFCON 660 (Edn 12/15) - Official-Sensitive Security Requirements
DEFCON 694 (Edn 07/21) - Accounting For Property of the Authority

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

DEFFORM 532 Personal Data Particulars

2d. Call-Off Charges

Capped Time and Materials (CTM)	☐
Incremental Fixed Price	☐
Time and Materials (T&M)	☒
Fixed Price	☐
A combination of two or more of the above Charging methods	☐
T&S is applicable	☐

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

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

Requirement Holder's Invoice Address
Ministry of Defence
DBS Finance
Walker House, Exchange Flags
Liverpool, L2 3YL
Website is: https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement
Phone: 0151-242-2000
Fax: 0151-242-2809

Requirement Holder's Authorised Representative
Ministry of Defence
DBS Finance
Walker House, Exchange Flags
Liverpool, L2 3YL
Website is: https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement
Phone: 0151-242-2000
Fax: 0151-242-2809

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

Statements of Works will be commissioned and agreed through the Contract Period.

Milestone/ Stage Payment number	Key Deliverable	Due Date	%	Milestone Payment value £ (ex VAT)
1				
2				
FINAL Payment	Satisfactory delivery and final acceptance of all work in providing the Deliverables. *(This final payment should include any costs held as retention based on % of the total cost.)*			
		Total Contract Value		

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

N/A

2i. Requirement Holder's Security Policy

Appendix 6 – Security Aspects Letter
Where applicable, a Security Aspects Letter should be issued and executed alongside this Order Form.

2j. Progress Reports and meetings

Progress Report Frequency	Monthly, the first Monday of each month	Progress Meeting Frequency	Monthly, the first Wednesday of each month

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

Not applicable	☐

2l. Key Staff

Not Applicable

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

2m. Key Subcontractor(s)

Not Applicable

2n. Commercially Sensitive Information

Supplier's Commercially Sensitive Information as per Appendix 9.

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).	☒

2p. Implementation Plan

Not applicable	☐

3. Charges

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

£7,680,000.00

4. Additional Insurances

Not applicable.

5. Guarantee

Not applicable.

6. Social Value Commitment

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)]

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

7. Requirement Holder Commercial Officer Authorisation

Order Form approved by (Name in capital letters)	Redacted Under FOIA Section 40, Personal Information	Telephone	Redacted Under FOIA Section 40, Personal Information
Directorate / Division	HOCS	Email	Redacted Under FOIA Section 40, Personal Information
Organisation Role / Position	Senior Commercial Officer	Date	01/05/2024
Approver's signature	Redacted Under FOIA Section 40, Personal Information		

8. Acknowledgement by Supplier

Order Form acknowledged by (Name in capital letters)	Redacted Under FOIA Section 40, Personal Information	Telephone	Redacted Under FOIA Section 40, Personal Information
Supplier Name	**Capgemini UK plc**	Email	Redacted Under FOIA Section 40, Personal Information
Supplier Role / Position	**Executive Vice President**	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

DEFFORM 111
(Edn 10/22)

Appendix 1 - Addresses and Other Information

1. Commercial Officer
Name: Redacted Under FOIA Section 40, Personal Information

Address: Main Building, Whitehall, London SW1A 2HB

Email: **Redacted Under FOIA Section 40, Personal Information**

☎

2. Project Manager, Equipment Support Manager or PT Leader (from whom technical information is available)
Name: **Redacted UnderFOIA Section 40, Personal Information**

Address

Email:

☎

3. Packaging Design Authority
Organisation & point of contact:
not applicable

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

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

See box 2

5. Drawings/Specifications are available from
not applicable

6. Intentionally Blank

7. Quality Assurance Representative:

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

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

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

10. Transport. The appropriate Ministry of Defence Transport Offices are:
A. DSCOM, DE&S, DSCOM, MoD Abbey Wood, Cedar 3c, Mail Point 3351, BRISTOL BS34 8JH
Air Freight Centre
IMPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943
EXPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943
Surface Freight Centre
IMPORTS ☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946
EXPORTS ☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946
B. JSCS

JSCS Helpdesk No. 01869 256052 (select option 2, then option 3)
JSCS Fax No. 01869 256837
Users requiring an account to use the MOD Freight Collection Service should contact UKStratCom-DefSp-RAMP@mod.gov.uk in the first instance.

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

12. Forms and Documentation are available through *:
Ministry of Defence, Forms and Pubs Commodity Management
PO Box 2, Building C16, C Site
Lower Arncott
Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)
Applications via fax or email:
Leidos-FormsPublications@teamleidos.mod.uk

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

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].

4. 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

Redacted Under FOIA Section 43, Commercial Interests

Appendix 3

Where applicable, the first Statement(s) of Works shall be inserted into this Appendix 3 as part of the executed Order Form. Thereafter, the Requirement Holder and Supplier may complete and execute Statement of Works (in the form of the template Statement of Work in Appendix 4 to Framework Schedule 6 (Order Form Template, Statement of Work Template)).

Appendix 4 (Template 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 Contact.

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:

SOW Reference:

Call-Off Contract Reference:

Requirement Holder:

Supplier:

SOW Start Date:

SOW End Date:

Duration of SOW:

Key Personnel (Requirement Holder):

Key Personnel (Supplier):

Subcontractors:

2. Call-Off Contract Specification – Deliverables Context

SOW Deliverables Background: [Insert details of which elements of the Deliverables this SOW will address]

Delivery phase(s): [Insert item and nature of Delivery phase(s), for example, Discovery, Alpha, Beta or Live]

Overview of Requirement: [Insert details including Release Type(s), for example Ad hoc, Inception, Calibration or Delivery]

3. Requirement Holder Requirements – SOW Deliverables

Outcome Description:

Milestone Ref	Milestone Description	Acceptance Criteria	Due Date
MS01			
MS02			

Delivery Plan:

Dependencies:

Supplier Resource Plan:

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).

[If different security requirements than those set out in the Contract apply under this SOW, these shall be detailed below and apply only to this SOW:

[**Insert** different security requirements if necessary] **]**

SOW Standards:

[Insert any specific Standards applicable to this SOW]

Performance Management:

[**Insert** details of Material KPIs that have a material impact on Contract performance]

The following Material KPIs shall apply in accordance with Framework Schedule 4 (Framework Management):

Material KPIs	Target	Measured by

[**Insert** Service Levels and/or KPIs – See Call-Off Schedule 14 (Service Levels)]

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	Contract Details	Employment / Engagement Route **(incl. inside/outside IR35)**

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 regularity of Submission
1.	[insert]		
1.1	[insert]	[insert]	[insert]

4. Charges

Call Off Contract Charges:

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

- [Capped Time and Materials]
- [Incremental Fixed Price]
- [Time and Materials]
- [Fixed Price]
- [2 or more of the above charging methods]

[Requirement Holder to select as appropriate for this SOW]

The estimated maximum value of this SOW (irrespective of the selected charging method) is **£[Insert detail].**

Rate Cards Applicable:

[Insert SOW applicable Supplier and Subcontractor rate cards from Call-Off Schedule 5 (Pricing Details and Expenses Policy), including details of any discounts that will be applied to the work undertaken under this SOW.]

Reimbursable Expenses:

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

[Reimbursable Expenses are capped at **[£[Insert]** [OR **[Insert]** percent ([**X**]%) of the Charges payable under this Statement of Work.]

[None]

[**Requirement Holder** to delete as appropriate for this SOW]

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:

Title:

Date:

Signature:

For and on behalf of the Requirement Holder

Name:

Title:

Date:

Signature:

Annex 1 to Statement of Work

Data Processing

Joint Schedule 11 (Processing Data) is replaced by

- DEFCON 532B (Edn. 12/22) Protection Of Personal Data (Where Personal Data is being processed on behalf of the Authority) and
- DEFFORM 532 Personal Data Particulars in appendix 8.

Appendix 5

Confidentiality Undertaking

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 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

For the attention of:

Redacted UnderFOIA Section 40, Personal Information

ITT/CONTRACT NUMBER & TITLE: 710422450 Automation Garage (AG) Analysis, Innovation and Development

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 OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition[1] outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
Existence of project.	OFFICIAL
Business card level details (e.g. names, roles, business email, etc).	OFFICIAL
Project plans, milestones, progress reports, agendas, minutes of meetings, general client correspondence.	Up to OFFICIAL-SENSITIVE
Information contained on any Ministry of Defence Systems, including personal data.	Up to OFFICIAL-SENSITIVE
Information on current and future defence technical capabilities, designs and infrastructure.	Up to OFFICIAL-SENSITIVE
Draft versions of any Ministry of Defence or Other Government Department strategies, policies and/or guidance.	Up to OFFICIAL-SENSITIVE
Information on any other topics that are related, indirectly related and/or not related to current and future military technical capabilities, Whole Force and infrastructure.	Up to OFFICIAL-SENSITIVE
Civilian and Service Personnel data	OFFICIAL–SENSITIVE PERSONAL

(Note: Add more rows as required)

3. Your attention is drawn to the provisions of the Official Secrets Act 1911-1989 in general, and specifically to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989). In particular you should take all reasonable steps to make sure that all individuals

[1] Annex C - Contractual Security Conditions

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 information shall be protected in accordance with applicable national laws and regulations.]

d. All employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this 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 Officer in accordance with DEFCON 76.

Yours faithfully

Copy via email to:
ISAC-Group (MULTIUSER)
COO-DSR-IIPCSy (MULTIUSER)
UKStratComDD-CyDR-CySAAS-021

ANNEX to Security Aspects Letter

1.1. *UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS*

Issued 10 July 2023

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 marking 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 requirements specified in ISNs, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

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

https://www.dstan.mod.uk/toolset/05/138/000003000.pdf
https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

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

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

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

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

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

Access

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

14. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE material have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

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

Hard Copy Distribution

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

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

Electronic Communication and Telephony and Facsimile Services

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

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

Details of the CPA scheme are available at:
https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

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

19. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so.

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

Use of Information Systems

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Unauthorised access to this computer system may constitute a criminal offence"

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

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

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

Laptops

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

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites[2]. 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

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

Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD Defence Industry WARP will also advise the Contractor what further action is required to be undertaken.

UK MOD Defence Industry WARP Contact Details
Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)
RLI Email: defencewarp@modnet.r.mil.uk (MULTIUSER)
Telephone (Office hours): +44 (0) 30 6770 2185
Mail: Defence Industry WARP, DE&S PSyA Office
MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

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

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

Sub-Contracts

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

33. The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a sub-Contractor facility located in another (third party) country. The first page of Annex A (MOD Form 1686 (F1686) of ISN 2023/06 is to be used for seeking such approval. The MOD Form 1686 can be found at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1162250/ISN_2023-06_Subcontracting_or_Collaborating_on_Classified_MOD_Programmes.pdf

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

Physical Destruction

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

Private Venture Activities

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

- Variants. Variants of standard defence equipment under research, development or in production, e.g., aircraft, military vehicles or ships, etc. with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of an item in-Service with UK Armed Forces;

- Derivatives. Equipment for military or civil use that is not based on standard Service designs but is dependent upon expertise or technology acquired in the course of defence contracts;

- Freelance. Equipment of defence importance that is in no way based on information gained from defence contracts;

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

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

Publicity Material

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

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

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

Export sales/promotion

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

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

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

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

Interpretation/Guidance

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

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

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

Audit

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

Appendix 7

Statement of Requirements

DEFENCE BUSINESS SERVICES AUTOMATION GARAGE – ANALYSIS, INNOVATION AND DEVELOPMENT

Introduction / Background	
A description of the organisation and a description of the work undertaken	Defence Business Services (DBS) is one of the largest shared service organisations in Europe that provides a wide range of corporate services to over 1.2 million end users, including serving and past military and families, as well as MOD civil servants and industry. DBS delivers large scale administration and smaller specialist services to enable the wider MOD to focus on its core aims, maintaining the UK's Defence and Security. Services including Human Resources, Pay, Veterans, Finance and Procurement. The Defence Business Service (DBS) Digital, Information and Technology (DIT) Automation Garage (AG) is a DevOps capability delivering innovation, automated and digital solutions, modernising legacy processes across Corporate Finance, HR and Armed Forces and Veterans to modernise manual processes, utilised by 50K civilians and 200K military personnel.
A description of the requirement	The Supplier will provide the following Services which are to be captured in the Proposals: actual Services to be provided by the Supplier to the Buyer will be specified and agreed in SoWs. The Buyer requires the Supplier to help the Buyer to: o build upon the existing automation and digitalisation capabilities across Defence and provide best practice advice and support to ensure automation and digitalisation is built in a coherent and efficient manner; o support the objectives of the Buyer's Automation Garage in Defence to: o Promote automation and digitalisation of services o Increase coherence o Make automation and digitisation benefits-driven o Increase automation and digital skills across Defence; o help create a showcase for automation and digitalisation across Defence – using the most effective communications and events to promote and help staff actively support automation and digitalisation activities and the benefits associated with it; o bring external expertise and experience – including industry case studies – to demonstrate longer term potential for automation and digitalisation in Defence; o understand future trends in the technology and the capacity for these to be deployed in Defence. Support the delivery of automation and digital technologies aligned with the DBS AG three-year roadmap;

	○ support the delivery of hyper automation technologies (including machine learning and cognitive/AI tools) and individual automations through the lifecycle including the Power Platform, preferred intelligent business process management (iBPM) technologies, preferred robotic process automation technologies (including Blue Prism) and others as the Buyer's strategy develops; ○ support the development of the DBS AG workstreams including: technology platforms, automation delivery and live services, public facing services on gov.uk, benefits, user-centred design, learning & development, technical policy, support, and communications and engagement; ○ support the development of automation and digital strategies and plans for Buyer business areas; ○ provide resources to analyse, develop and deploy specific automations and digital products on behalf of Defence; and ○ provide upskilling and knowledge transfer in automation and digital technologies utilised in the Automation Garage to in-house AG staff.
Performance/Quality requirements	No specific Quality Management System requirements are defined. This does not relieve the Supplier of providing conforming products under this contract. The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: The Technology Code of Practice - GOV.UK (www.gov.uk) The Supplier will comply with the GDS Service Standard and Defence Service Manual - Design great digital services - Defence Service Manual (defence-service-manual.netlify.app), as applicable.
Deliverables	The below are example of deliverables through the contracted supplier. These deliverables are non-exhaustive and un-prioritised and will be mapped against Statements of Work through the Time and Materials contract: i. Skills under the following Job Families: a. Technical b. Product and Delivery c. Quality Assurance Testing (QAT) d. IT Operations e. User Centred Design f. Data Scientists g. Performance Analyst ii. Upskilling Tracker - Knowledge Transfer and Skills Transfer from the supplier to the internal team

	iii. Automation Garage Operating Model iteration and implementation - Iterate and continually grow the AG operating model to align with Defence priorities and Government Digital Services (GDS) standards. Ensuring the AG are able to deliver digital products to increase productivity and efficiency across DBS and wider MOD. This must enable scalability and fast flow of digital products. iv. Innovation - Develop and cohere innovation activity in the Digital sphere across DBS, aligned with AG three-year roadmap, driving innovation into enabling the Digital Transformation Programme. v. Review of extant Benefits frameworks in use by DBS and provide a suitable benefit mapping and realisation model for Automation Garage to effectively manage benefits. vi. Project Plans, with milestones where relevant, for individual Statement of Work where directed
Location (where the work/task is to be performed)	The Services will be delivered to DBS DIT Automation Garage, Oak, East 1, Abbeywood North, Bristol, BS34 8QW. Recognising the hybrid ways of working adopted by the MOD, the Services will be delivered remotely and/or to: • Abbeywood North, Bristol, BS34 8QW; • Norcross, Thornton Cleveleys, Lancashire, FY5 3WP; and • HMS Sultan, Centurion Building, Gosport, PO13 9XA. Detail of hybrid working arrangements will be agreed within each SOW. The primary location for any face-to face Services will be at one of the above locations, or as agreed between the Supplier and Buyer.
Technical Publications, if required	N/A
Qualifications/experience required	Suitable qualified and experienced people (SQEP), aligned with Digital, Data and Technology (DDaT) framework and DIPs Lot 2 Skill Requirements.
Training/skill transfer	Knowledge Transfer and Skills Transfer from the supplier to the internal team, to be completed throughout the period of the contract, which will be monitored using an upskilling tracker. This upskilling tracker will be created collaboratively as part of the work package. Regular knowledge transfer sessions are expected, between the Supplier resources and existing and new Buyer in-house resources, to ensure Buyer in-house staff understanding of unique build requirements following Supplier off-boarding, with training and knowledge documentation also being created for use by newly recruited Buyer in-house staff

<table>
<tr><td>Delivery details</td><td>All services to be delivered between the hours of 0700 to 1900 on weekdays with exception of recognised UK Bank Holidays and Public Holidays.</td></tr>
<tr><td>Acceptance criteria</td><td>The Supplier undertakes that all Services will meet the Buyer’s acceptance criteria, as defined in the individual Statement of Works.</td></tr>
<tr><td>Government furnished resources/equipment</td><td>The Buyer’s equipment to be used with this Call-Off Contract includes:
Managed credentials and managed end user devices (MODNET laptops) with collaborative tools to access, create and modify resources classified up to OFFICIAL-SENSITIVE;
Managed credentials to access MODCloud ACE accounts;
Managed credentials to access MOD collaboration platforms (Google Workspace, Slack, Jira, GitHub etc)
Physical Site Access Passes as required
Managed credentials to access Mandatory Training courses required to enable full Supplier resource onboarding activities to take place.</td></tr>
<tr><td>Reporting/review/progress issues</td><td>Where Supplier resources are utilised, the Buyer will monitor the deliveries against the estimated development timescales and seek to address any dips in performance through replacement of resources with more highly skilled individuals; understanding of technological constraints; or a reduction in contract value.

Monthly Supplier Performance Sessions will also be held between Buyer's Programme Managers and External Support Leads to discuss:
Statement of Works
Performance measured in accordance with, but not limited to, the KPI table listed below
Recommendations for new and innovated ways of working.
<table>
<tr><th>KPI</th><th>KPI Description</th><th>Target</th></tr>
<tr><td>1</td><td>Supplier to ensure that where a Tasking Note is on a T&M basis the estimate is accurate to within 10% of the total cost but is not exceeded</td><td>95%</td></tr>
<tr><td>2</td><td>Supplier to successfully secure required resource within 4 weeks of placement of request</td><td>95%</td></tr>
<tr><td>3</td><td>Upskilling 10 full time equivalent employees per annum, to the level of Proficient against the DDaT Capability Framework criteria</td><td>100%</td></tr>
</table></td></tr>
</table>

	In the event that the Contractor falls below the stated % Targets then they will be expected to provide a Rectification Plan to Head Office Commercial within 7 days, detailing the actions they will take to restore the expected % Targets in time for the next Monthly Performance Review Meeting
Management information	N/A
Security Clearance requirements	The Supplier is to ensure that all of the Suppliers' Personnel have Security Check (SC) clearance. Where the Supplier's Personnel does not have SC clearance that individual will not be allowed access to MOD facilities or data. All information related to or generated by this Contract is to be treated in the appropriate manner in accordance with Government Security Classifications and is proprietary to the Automation Garage. The classification of the material to be handled shall not exceed OFFICIAL-SENSITIVE in nature. All personal data processed under this Contract is to be treated in accordance with the Data Protection Act 2018.

Appendix 8

Personal Data Particulars

DEFFORM 532
Edn 10/19

This Form forms part of the Contract and must be completed and attached to each Contract containing DEFCON 532B.

Data Controller	The Data Controller is the Secretary of State for Defence (the Authority). The Personal Data will be provided by: Defence Business Services, Digital and Information Technology, Automation Garage, Oak, East 1, Abbeywood North, Bristol, BS34 8QW
Data Processor	The Data Processor is the Contractor. The Personal Data will be processed at: MOD sites located in Bristol, Norcross, Gosport or on MOD Laptops
Data Subjects	The Personal Data to be processed under the Contract concern the following Data Subjects or categories of Data Subjects: End users/customers of all the applications utilised in automation and digital solutions. This could include Staff (including civilian and Service personnel, volunteers, agents and temporary workers), customers/clients, suppliers, patients, students/pupils, members of the public, users of a particular website, etc, will be the subject or categories of data subjects
Categories of Data	The Personal Data to be processed under the Contract concern the following categories of data: Representatives of Customer: name, address, email address, billing information, login credentials, geolocational data, professional affiliation, financial data, supplier data List is not exhaustive
Special Categories of data (if appropriate)	The Personal Data to be processed under the Contract concern the following Special Categories of data: Religious and health data
Subject matter of the processing	The processing activities to be performed under the contract are as follows: Suppliers should not need to directly access or process live personal data as they will be working within development and test environments which will contain obfuscated data, but it is possible they may require access to live date in certain limited scenarios. In this sense the subject matter of the processing would be the users of the automation or digital product in question.
Nature and the purposes of the Processing	The Personal Data to be processed under the Contract will be processed as follows: Suppliers should not need to directly access or process live personal data as they will be working within development and test environments which will contain obfuscated data, but it is possible they may require access to live date in certain limited scenarios. The nature and purpose of the processing would be related to the specific automation or digital product being developed, and could include the

	collection, recording and use of data for the purpose of completion transactions to deliver civilian or military processes such as invoicing, update of records within the MyHR or Commercial, Procurement and Finance systems.
Technical and organisational measures	The following technical and organisational measures to safeguard the Personal Data are required for the performance of this Contract: Suppliers should not need to directly access or process live personal data as they will be working within development and test environments which will contain obfuscated data, but it is possible they may require access to live date in certain limited scenarios. Where access the live personal data is required, this would be via authorisation by DBS Data Protection Team, granting access to the required system for a limited time and scenario, with access being revoked on immediate completion of the work.
Instructions for disposal of Personal Data	The disposal instructions for the Personal Data to be processed under the Contract are as follows (where Disposal Instructions are available at the commencement of Contract): If personal data is to be processed, it will be during the development and testing phase of an individual process. The disposal instructions for any live personal data will be
Date from which Personal Data is to be processed	Where the date from which the Personal Data will be processed is different from the Contract commencement date this should be specified here: A date from which personal data is to be processed cannot be determined until such time as the AG is requested to deliver a new automation or digital product, which would require the use of live personal data, as obfuscated data is used in the majority of all development and testing activities. This need would be identified as part of the Discovery phase for this individual requests.

The capitalised terms used in this form shall have the same meanings as in the General Data Protection Regulations.

Appendix 9

DEFFORM 539A
Edn 01/22

Tenderer's Sensitive Information

This list shall be agreed in consultation with the Authority and the Contractor and may be reviewed and amended by agreement. The Authority shall review the list before the publication of any information.

ITT Ref No:710422450
Description of Tenderer's Sensitive Information: Redacted Under FOIA Section 43, Commercial Interests
Cross Reference(s) to location of Sensitive Information in Tender: Redacted Under FOIA Section 43, Commercial Interests
Explanation of Sensitivity: Redacted Under FOIA Section 43, Commercial Interests
Details of potential harm resulting from disclosure: Redacted Under FOIA Section 43, Commercial Interests
Period of Confidence (if applicable): Redacted Under FOIA Section 43, Commercial Interests
Contact Details for Transparency / Freedom of Information matters: Name: Redacted Under FOIA Section 43, Commercial Interests Position: Data Protection Officer Address: Redacted Under FOIA Section 43, Commercial Interests Telephone Number: Redacted Under FOIA Section 43, Commercial Interests Email Address: Redacted Under FOIA Section 43, Commercial Interests