

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

Order Form

1a. Identification

Call-Off Lot	Lot 1				
Call-Off Reference	RM6249/DIPS PS 503	Version Number	1.0	Date	26/09/2024
Business Case Reference	Original FBC Number				
	Amendment FBC Number	Not Applicable			
Project / equipment for which Services are in support	MNO Core Team	Urgent Capability Requirement (UCR)		Not Applicable	

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

Call-Off Contract title:	PS 503 – MNO Core Team
--------------------------	------------------------

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.

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









Call-Off Contract description:	<ul style="list-style-type: none">• Provide Technical Authority for MNO programme to ensure the MNO Programme delivers required outputs to MOD.• Management of the Design and Implementation of the MNO Interim Support Service to ensure the MNO Programme delivers required outputs to MOD.
1b. Contact details	

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.

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

Government Directorate / Organisation Title	MNO Core Team	Name of Supplier	<i>Eviden Technology Services Limited</i>
Name of Requirement Holder's Authorised Representative		Name of Supplier's Authorised Representative	
Post title	End User Services - Service Executive	Post title	<i>Client Executive Partner - Defence</i>
Requirement Holder's Address		Supplier Address	<i>Eviden Technology Services Limited a company registered under the laws of Jersey with registration number 146917 and whose registered address is at 44 Esplanade, St Helier Jersey, JE4 9WG, which operates through its UK establishment, Eviden Technology Services Limited, which is registered in England and Wales under number BR025381 and whose registered office is at Second Floor, Mid City Place, 71 High Holborn, London, WC1V 6EA.</i>
Postcode	Defence Digital, Strategic Command, Spur F2, Bldg 405, MoD Corsham, Westwells Rd, Wiltshire SN13 9NR	Postcode	
Telephone		Telephone	
Email		Email	
Unit Identification Number (UIN)	D8001H D1899A	Value Added Tax (VAT) Code	GB232327983
Resource Accounting Code (RAC)	NPB052		
Name of Requirement Holder's Project Lead			
Requirement Holder's Secondary Contact Name		Supplier Secondary Contact Name	

OFFICIAL SENSITIVE (when complete)

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

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	26/09/2024	Deadline for Requirement Holder's receipt of Supplier's Call-Off Tender	26/09/2024
---	------------	--	------------

1c. Statement of Requirements (SOR) (This section 1c. to be completed in full OR a complete SOR to be attached in Appendix 7 of this document)			
Unique Order Number (defined by delivery team)	n/a		
SOR version issue number	1.0	SOR dated	19/08/2024
SOR title	20240819 - MNO Core Team Requirements v1.0 - OS		

Background/justification for Call-Off Contract				
<ul style="list-style-type: none">Provide Technical Authority for MNO programme to ensure the MNO Programme delivers required outputs to MOD.Management of the Design and Implementation of the MNO Interim Support Service to ensure the MNO Programme delivers required outputs to MOD.				
Description of Services to be provided under the Call-Off Contract				
Provide Technical Authority for MNO programme to ensure the MNO Programme delivers required outputs to MOD.				
Activities required to be undertaken under the Call-Off Contract				
Output 1	Architecture – Until 31 st Dec 2025	Provide Technical Authority for MNO programme to ensure the MNO Programme delivers required outputs to MOD.		Acceptance Criteria
Output 1.1	Architecture – Governance	Lead TAB and design review processes	Technical Assurance Board Arranged (TAB) Technical Design Decision Register created and published. TAB minutes and actions published.	None

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

Output 1.2	Architecture – Assurance	Lead work to ensure that HLD/LLDs are updated (by other suppliers) and approved as required to align with the TDA endorsed MNO	HLDs and LLDs recorded as approved at MNO Technical Assurance Board.	Suppliers to make HLDs and LLDs available for review. Suppliers to reissue HLDs and LLDs post
------------	--------------------------	--	--	--

		solution, approaches and patterns		review for final approval
Output 1.3	Architecture - Assurance	Take technical solutions to TDA for approval as required. Attendance on TDA to determine impact of other suggested architectural activity on MNO	HLDs recorded as approved by – or on behalf of – TDA. Recorded attendance at weekly TDA.	TDA – or representative of TDA – to provide final approval
Output 2	Service Management - Until 31 st July 2025	Management of the Design and Implementation of the MNO Interim Support Service to ensure the MNO Programme delivers required outputs to MOD.		Acceptance Criteria

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

Output 2.1	Service Management	ITSM (service tooling) and MAM (platform monitoring tooling) plans – including milestones, activities, resource requirements and costs - are in place.	ITSM & MAM Plan – updated weekly and shared during Service Management bi-weekly calls	OSM engagement & onboarding team availability Supplier SMEs availability	
Output 2.2	Service Management	Interim Service Management SDP (Service Design Pack) – describing how the 500 user Pilot user group and MNO services, will be supported, monitored, and managed.	Published MNO SDP V1	OSM engagement & onboarding team availability Supplier SMEs availability	
Output 2.3	Service Management	Interim ITSM Process workflows – including Incident, Problem, Config, knowledge, Change and Request Interim Swivel Chair solution – describing the processes for transfer and management of tickets between the MNO Interim Service Management team and suppliers.	Version 1 ITSM Process workflows published	OSM engagement & onboarding team availability Supplier SMEs availability	

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

Output 2.4	Service Management	OSM T3 Onboarding Complete OSM onboarding for Incident, Knowledge & SACM meeting Operational Acceptance Criteria (OAC)	OSM OAC and approval Gate Ready to Test achieved	OSM engagement & onboarding team availability Supplier SMEs availability
Output 2.5	Service Management	Interim Monitoring and Management (MAM) SDP – describing how the MNO services will be monitored and managed by the MNO programme and	MAM SDP V1 published	OSM engagement & onboarding team availability Supplier SME availability

		feeding into the Authority's event and security solutions.			
--	--	--	--	--	--

Output 2.6	Service Management	Event Management OAC met ready for OSM onboarding - including Event Mgt plan detailing the MAM Event requirements, connectivity, thresholds, and service performance measures for the MNO service.	OSM Approval – Ready to Test Gate achieved	OSM engagement & onboarding team availability Supplier SME availability Authority Event management team OSM Event management MDS and ICD documents available
2.7	Service Management	Support the ITSM until handover to new supplier		

Outputs to be provided under the Call-Off Contract

See "Authority's Desired Outcome" identified in the Table above.

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

Acceptance/rejection criteria / provisions
See "Minimum Service Requirements" identified in the Table above.
Material KPIs / Critical Service Level Failure
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 CallOff 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
Buyer to provide laptops with access to MODNET to enable the delivery of the service.
Additional quality requirements & standards (in addition to any quality requirements & standards detailed in the addition to the Call-off Schedules)
From the Call-Off Start Date, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards, including those referred to in Framework Schedule 1 (Specification). The Requirement Holder requires the Supplier to comply with the following additional Standards for this Call-Off Contract:
<ul style="list-style-type: none"> 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
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	1 October 2024
Call-Off Initial Period	15 Months
Call-Off Expiry Date	31 December 2025
Call-Off Optional Extension Period	2 Months
Minimum notice period prior to a Call-Off Optional Extension Period	One Month

SOR approved by (Name in capital letters)		Telephone	
Directorate / Division	Defence Digital	Email	
Organisation Role / Position	End User Services - Service Executive	Date	26/09/2024
Approver's signature			

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

				Original FBC Number	Amendment FBC
1d. Key Deliverables Template					
Output 2.3	Service Management	Interim ITSM Process workflows – including Incident, Problem, Config, knowledge, Change and Request Interim Swivel Chair solution – describing the processes for transfer and management of tickets between the MNO Interim Service Management team and suppliers.	Version 1 ITSM Process workflows published	OSM engagement & onboarding team availability Supplier SMEs availability	
Output 2.4	Service Management	OSM T3 Onboarding Complete OSM onboarding for Incident, Knowledge & SACM meeting Operational Acceptance Criteria (OAC)	OSM OAC and approval Gate Ready to Test achieved	OSM engagement & onboarding team availability Supplier SMEs availability	
Output 2.5	Service Management	Interim Monitoring and Management (MAM) SDP – describing how the MNO services will be monitored and managed by the MNO programme and feeding into the Authority's event and security solutions.	MAM SDP V1 published	OSM engagement & onboarding team availability Supplier SME availability	
Output 2.6	Service Management	Event Management OAC met ready for OSM onboarding - including Event Mgt plan detailing the MAM Event	OSM Approval – Ready to Test Gate achieved	OSM engagement & onboarding team availability Supplier SME availability	

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

		requirements, connectivity, thresholds, and service performance measures for the MNO service.		Authority Event management team OSM Event management MDS and ICD documents available
2.7	Service Management	Support the ITSM until handover to new supplier		

2. Call-Off Incorporated Terms

OFFICIAL-SENSITIVE - COMMERCIAL
OFFICIAL SENSITIVE (when complete)

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

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

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] Not Applicable
- 5 The following Schedules in equal order of precedence:
 - Joint Schedules ○ Joint Schedule 2 (Variation Form) ○ Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information) ○ Joint Schedule 5 (Corporate Social Responsibility) ○ Joint Schedule 10 (Rectification Plan) ○ Joint Schedule 11 (Processing Data)
 - Call-Off Schedules ○ Call-Off Schedule 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 9 (Security) ○ Call-Off Schedule 10 (Exit Management) ○ Call-Off Schedule 13 (Implementation Plan and Testing)

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

- Call-Off Schedule 26 (Cyber)

6 Core Terms (DIPS version)

7 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Requirement Holder (as decided by the Requirement Holder and Commercial) take precedence over the documents above.

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

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

2a. Strategy for procurement and evaluation

Further competition	<input type="checkbox"/>	Competitive award criteria to be used for undertaking evaluation of proposal(s)	Direct Award		
Direct award	<input checked="" type="checkbox"/>				
		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:

- 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.
- A minimum of SC clearance is required for all supplier staff working on this contract.

☐

2c. Call-Off Special Terms

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

None

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

2d. Call-Off Charges			
Capped Time and Materials (CTM)			
Incremental Fixed Price			
Time and Materials (T&M)			
Fixed Price	X		
A combination of two or more of the above Charging methods			
T&S is applicable			
No T&S is available			
Reimbursable Expenses			
None			

2e. Payment Method			

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



CP&F payment.

PO Number TBA

Requirement

Holder's

Invoice

Address

[Redacted]

End User Services - Service Executive

[Redacted]

[Redacted]

Defence Digital, Strategic Command, Spur F2, Bldg 405, MoD Corsham,
Westwells Rd, Wiltshire SN13 9NR

Requirement Holder's Authorised Representative

[Redacted]

End User Services - Service Executive

[Redacted]

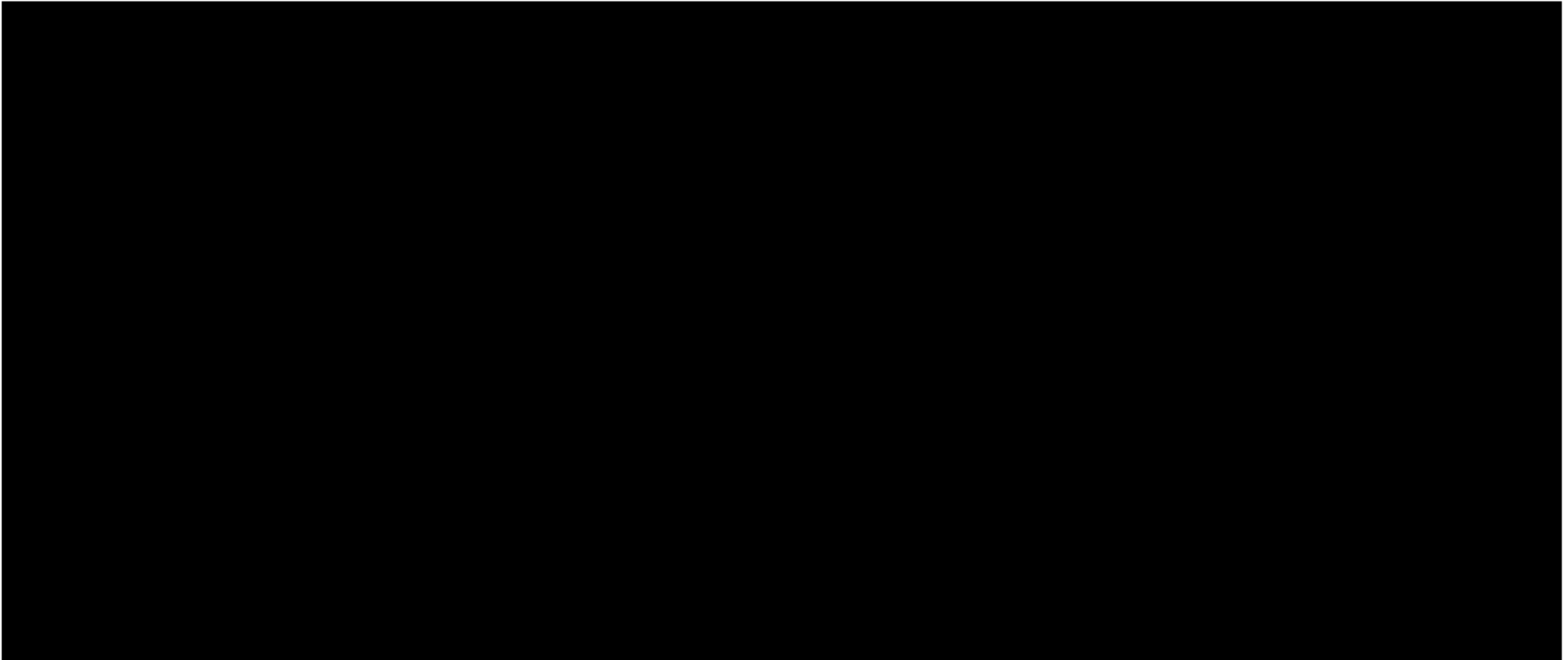
Defence Digital, Strategic Command, Spur F2, Bldg 405, MoD Corsham,
Westwells Rd, Wiltshire SN13 9NR

OFFICIAL-SENSITIVE - COMMERCIAL
OFFICIAL SENSITIVE (when complete)

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

Call Off Contract Charges:

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



Rate Cards Applicable: DIPS Lot 1 rate card

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. This equates to 125% of contract value.

2h. Requirement Holder's Environmental Policy

Available online at: [Management of environmental protection in defence \(JSP 418\) - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/management-of-environmental-protection-in-defence-jsp-418)

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

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)	<input type="checkbox"/>

DocuSign Envelope ID: 9AA7C1EA

Relevant MAA Regulatory Publications (See attachment for details)	<input type="checkbox"/>
Additional Quality Requirements (See attachment for details)	<input type="checkbox"/>
Planned maintenance schedule requirement	
Not applicable	<input type="checkbox"/>

2l. Key Staff

OFFICIAL SENSITIVE (when complete)

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

Supplier's Contract Manager: Steve Harris

2m. Key Subcontractor(s)

None

2n. Commercially Sensitive Information

Pricing

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**

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

Total cost £645,048.32 (Exc VAT)

Docusign Envelope ID: 9AA7C1EA

Not applicable

5. Guarantee

Not applicable

6. Social Value Commitment

Not applicable

4. Additional Insurances

OFFICIAL SENSITIVE (when complete)

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

7. Requirement Holder Commercial Officer Authorisation			
Order Form approved by (Name in capital letters)	[REDACTED]	Telephone	[REDACTED]
Directorate / Division	DD MOD	Email	[REDACTED]
Organisation Role / Position	[REDACTED]	Date	01/10/24
Approver's signature	[REDACTED]		












8. Acknowledgement by Supplier			
Order Form acknowledged by (Name in capital letters)	[REDACTED]	Telephone	[REDACTED]
Supplier Name	EVIDEN TECHNOLOGY SERVICES LIMITED	Email	[REDACTED]
Supplier Role / Position	[REDACTED]	Date	30.09.2024
Approver's signature	[REDACTED]		

DocuSign Envelope ID: 9AA7C1EA

9. Final Administration	
<p>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</p>	

Docusign Envelope ID: 9AA7C1EA-306F-4E9C-9F8A-D8921C05F59C

Appendix 1 - Addresses and Other Information

1. Commercial Officer Name: Address: 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 Finance 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: Email: 	9. Consignment Instructions The items are to be consigned as follows:
3. Packaging Design Authority Organisation & point of contact: (Where no address is shown please contact the Project Team in Box 2) 	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 <u>Air Freight Centre</u> IMPORTS  030 679 81113 / 81114 Fax 0117 913 8943 EXPORTS  030 679 81113 / 81114 Fax 0117 913 8943 <u>Surface Freight Centre</u> IMPORTS  030 679 81129 / 81133 / 81138 Fax 0117 913 8946 EXPORTS  030 679 81129 / 81133 / 81138 Fax 0117 913 8946 B.
4. (a) Supply / Support Management Branch or Order Manager: Branch/Name:  (b) U.I.N.	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 UKStratComDefSpRAMP@mod.gov.uk in the first instance.
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/ministryofdefence/about/procurement

DocuSign

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

Appendix 1 to Schedule 6

OFFICIAL SENSITIVE (when complete) 19

DocuSign Envelope ID: 9AA7C1EA-306F-4E9C-9F8A-D8921C05F59C

helpdesk visit <http://dstan.gateway.isg-r.r.mil.uk/index.html>[intranet] or <https://www.dstan.mod.uk/> [extranet, registration needed]

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.

OFFICIAL SENSITIVE (when complete) 20

Appendix 2 to Schedule 6

DocuSign Envelope ID: 9AA7C1EA-306F-4E9C-9F8A-D8921C05F59C

Appendix 2 – Supplier's Quotation - Charges Summary Not Used (See Appendix 4)

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:

2. From:

Date of tender submission:

In response to the Order Form request for a quotation
reference

Dated

*The work can be undertaken and our detailed response is attached. ☐

*We are unable to provide the resources/deliverables identified on this occasion. ☐

(* Check box as appropriate)

Name: (Block Capitals)

Signed:

Date:

2. Call-Off title:

3. Supplier Unique Reference Number:

4. Start Date:

Completion Date:

5a. Manpower/Resources

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

5b. Travel

(Estimated expenditure on:)

Unit cost

Number of Journeys / Miles

Total

Rail

Motor Mileage
(max 30p per mile incl VAT)

30p max
(incl VAT)

Air

Sea

5c. Subsistence

(Estimated expenditure on:)

Unit cost

Number of Night / Days

Total

Accommodation
(max £100 per night incl VAT)

Meals (max £5 for lunch and/or
£22.50 for an evening meal,
including all drinks

Miscellaneous costs (please
define below)

The above T&S costs relate to the period to

	<u>Subcontractor price</u>	
5d.Other Costs		
	Subcontractor Details	
	Materials	
	Other (Please provide details below)	
	Description	Cost
Total Charges for completion of Call-Off Contract	(excl. VAT)
	Deliverables	

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

OFFICIAL SENSITIVE (when complete)

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 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: 19 Sep 24

SOW Title: MNO Core Team

SOW Reference: MNO Core Team SoR 19 Sep 24

Call-Off Contract Reference: RM6249/DIPS (05)024

Requirement Holder: TBC

Supplier: Eviden Technology Services Limited

SOW Start Date: 01 Oct 2024

SOW End Date: 31 Dec 2025

Duration of SOW: 15 months

SOW Extension Option 1 Start Date: 01 Jan 2026

SOW Extension Option 1 End Date: 28 Feb 2026

Duration of SOW Extension Option 1: 2 months

Key Personnel (Requirement Holder): Not applicable

Key Personnel (Supplier): Not applicable

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

Subcontractors: None

2. Call-Off Contract Specification – Deliverables Context

SOW Deliverables Background: The Authority requires additional programme management support to enable the ATLAS Exit Programme to achieve a coherent exit of the ATLAS contract and transition to new services.

Delivery phase(s): Not relevant for this SOW, as the phases are governed by the overall ATLAS Exit programme.

3. Requirement Holder Requirements – SOW Deliverables

OFFICIAL-SENSITIVE - COMMERCIAL

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

OFFICIAL SENSITIVE (when complete)

OFFICIAL-SENSITIVE - COMMERCIAL

Ref	Authority's Desired Outcome	Approach	Service requirement (monthly)	Acceptance Criteria
Output 1	Architecture – Until 28th Feb 2026	Provide Technical Authority for MNO programme to ensure the MNO Programme delivers required outputs to MOD.		
Output 1.1	Architecture – Governance	Lead TAB and design review processes	<p>Technical Assurance Board Arranged (TAB)</p> <p>Technical Design Decision Register created and published.</p> <p>TAB minutes and actions published.</p>	None
Output 1.2	Architecture – Assurance	Lead work to ensure that HLD/LLDs are updated (by other suppliers) and approved as required to align with the TDA endorsed MNO solution, approaches and patterns	HLDs and LLDs recorded as approved at MNO Technical Assurance Board.	<p>Suppliers to make HLDs and LLDs available for review.</p> <p>Suppliers to re-issue HLDs and LLDs post review for final approval</p>
Output 1.3	Architecture - Assurance	Take technical solutions to TDA for approval as required. Attendance on TDA to determine impact of other suggested architectural activity on MNO	<p>HLDs recorded as approved by – or on behalf of – TDA.</p> <p>Recorded attendance at weekly TDA.</p>	TDA – or representative of TDA – to provide final approval

Output 2	Service Management - Until 31st July 2025	Management of the Design and Implementation of the MNO Interim Support Service to ensure the MNO Programme delivers required outputs to MOD.
-----------------	---	---

Output 2.1	Service Management	ITSM (service tooling) and MAM (platform monitoring tooling) plans – including milestones, activities, resource requirements and costs - are in place.	ITSM & MAM Plan – updated weekly and shared during Service Management biweekly calls	OSM engagement & onboarding team availability Supplier SMEs availability
------------	--------------------	--	--	---

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

Output 2.2	Service Management	Interim Service Management SDP (Service Design Pack) – describing how the 500 user Pilot user group and MNO services, will be supported, monitored, and managed.	Published MNO SDP V1	OSM engagement & onboarding team availability Supplier SMEs availability
Output 2.3	Service Management	Interim ITSM Process workflows – including Incident, Problem, Config, knowledge, Change and Request Interim Swivel Chair solution – describing the processes for transfer and management of tickets between the MNO Interim Service Management team and suppliers.	Version 1 ITSM Process workflows published	OSM engagement & onboarding team availability Supplier SMEs availability

Output 2.4	Service Management	OSM T3 Onboarding Complete OSM onboarding for Incident, Knowledge & SACM meeting Operational Acceptance Criteria (OAC)	OSM OAC and approval Gate Ready to Test achieved	OSM engagement & onboarding team availability Supplier SMEs availability
Output 2.5	Service Management	Interim Monitoring and Management (MAM) SDP – describing how the MNO services will be monitored and managed by the MNO programme and feeding into the Authority's event and security solutions.	MAM SDP V1 published	OSM engagement & onboarding team availability Supplier SME availability
Output 2.6	Service Management	Event Management OAC met ready for OSM onboarding - including Event Mgt plan detailing the MAM Event requirements, connectivity, thresholds, and service performance measures for the MNO service.	OSM Approval – Ready to Test Gate achieved	OSM engagement & onboarding team availability Supplier SME availability Authority Event management team OSM Event management MDS and ICD documents available

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

2.7	Service Management	Support the ITSM until handover to new supplier		
-----	-----------------------	--	--	--

Dependencies:

- The Authority will provide MODNET access to the team to enable them to fulfil their obligations.
- The Authority will make available and support all reasonable requests to facilitate the discharge of our obligations and fulfil our deliverables.
- The Authority shall not unreasonably withhold or delay acceptance of deliverables.

Assumptions:

- 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. - The following will not be required due to the scope and size of the requirement:
 - o Quality plan o Exit plan o Disaster recovery and business continuity plan o Implementation plan and testing o Continuous improvement plan
- The requirement excludes any requirements for o Personal data processing o Additional quality assurance o Additional insurances

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).

All resources delivering the managed service will hold valid security clearances to SC and will sign a Confidentiality Undertaking.

SOW Standards: No specific standards are applicable

Performance Management: No KPIs or service levels identified for this SOW.

Additional Requirements: None identified

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

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:

Ref.	Type of Information	Which Deliverables does this requirement apply to?	Required regularity of Submission
1	Monthly Progress Report	All deliverables	Monthly

4. Charges

Basis of estimate:

Initial Contract										
		Daily Cost (ex VAT)	Oct-24	Nov-24	Dec-24	Jan-25	Feb-25	Mar-25	Apr-25	May-25
DIPS Lot 1 - B1/Grade 6	Architecture	£ 1,259.86	23	21	15	22	20	21	20	20
DIPS Lot 1 - B1/Grade 6	Service Management	£ 1,259.86	23	21	15	22	20	21	20	20

Initial Contract										
		Daily Cost (ex VAT)	Jun-25	Jul-25	Aug-25	Sep-25	Oct-25	Nov-25	Dec-25	

DIPS Lot 1 - B1/Grade 6	Architecture	£ 1,259.86	21	23	20	22	23	20	15	
DIPS Lot 1 - B1/Grade 6	Service Management	£ 1,259.86	21	23						

Extension Option

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

		Daily Cost (ex VAT)	Jan-26	Feb-26						
DIPS Lot 1 - B1/Grade 6	Architecture	£ 1,259.86	21	20						

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: Joel Smith

Title: Interim CEO UKI

Date: 30.09.2024

Signature:

Signed by:

joel smith

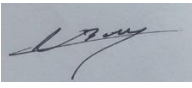
DAD38397BA1C4BE...

For and on behalf of the Requirement Holder

Name: Nick Barras

Title: Head of PS

Date: 1/10/24

Signature: 

Annex 1 to Statement of Work – Not Applicable

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
-------------	---------

<p>Identity of Controller for each Category of Personal Data</p>	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 of Joint Schedule 11 (Processing Data) and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> • [Insert the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority] <p>The Supplier is Controller and the Relevant Authority is Processor</p> <p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of Joint Schedule 11 (Processing Data) of the following Personal Data:</p> <ul style="list-style-type: none"> • [Insert the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier] <p>The Parties are Joint Controllers</p> <p>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> • [Insert the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together] <p>The Parties are Independent Controllers of Personal Data 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> <ul style="list-style-type: none"> • 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
--	---

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

Appendix 5 Confidentiality Undertaking

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

Employee:

Name of Employer:

MOD Contract/Task No:

Title:

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

Date of Issue: 17/09/2024

For the attention of:

Eviden Technology Service Limited
Second Floor, Mid City Place,
71 High Holborn
London,
WC1V 6EA

ITT/CONTRACT NUMBER xxx: SECURITY ASPECTS LETTER FOR MNO CORE TEAM.

1.

On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.
2.

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

ASPECTS		CLASSIFICATION
A.1 Existence of Project		OFFICIAL
A.2 Project/System Name		OFFICIAL
A.3 Details of delivery partners		OFFICIAL-SENSITIVE COMMERCIAL
A.4 High-Level Architecture summary/ Description of the project/system		OFFICIAL
A.5 Design Documentation	A.5.1 System Design Overview	OFFICIAL

	A.5.2 High Level Design (with no Ips or Aspects)	OFFICIAL
	A.5.3 Low Level Design Artefacts	OFFICIAL SENSITIVE
	A.5.4 Full complete set of HLDs or LLD artefacts	OFFICIAL SENSITIVE
A.6 Complete set of Design Documentation	A.6.1 Hardware and Software, logical and physical diagrams	OFFICIAL SENSITIVE
	A.6.2 Technical specification of hardware	OFFICIAL SENSITIVE
A.7 Network IP Addresses-Allocated to systems	A.7.1 A single IP address with no associated indication of its use, or the classification of the system or network on which it is being used	OFFICIAL

	A.7.2 A single or range of IP addresses, together with information that associates them as being used on a system or network either directly or by use of system or project names	OFFICIAL SENSITIVE
	A.7.3 The full IP range	OFFICIAL SENSITIVE
	A.7.4 Obfuscated IP address, single (e.g., x.x.1.1)	OFFICIAL
A.8 Audit and Accounting Data including collated events, alerts and logs (captured by firewalls, other gateways, servers and dedicated IDS/SIEM appliances)		OFFICIAL SENSITIVE
A.9 User Requirements Document	A.9.1 Complete document, linked to system capability	OFFICIAL SENSITIVE
A.10 Security documentation	A.10.1 Including risk assessments, RMADS, Security Aspects of the Design documentation and SWG minutes	OFFICIAL SENSITIVE
	A.10.2 Security Operating Procedures	OFFICIAL SENSITIVE
A.11 Management Documentation and Plans	A.11.1 Very high-level programme status information with no detail of purpose or role of system- ideally as a small part of wider reporting	OFFICIAL
	A.11.2 Very high-level financial information	OFFICIAL-SENSITIVE COMMERCIAL

	A.11.3 Scheduling information	OFFICIAL-SENSITIVE COMMERCIAL
A.12 Hardware Assets. All carry the same security classification as that of the network they are a part of or have been used on.	A.12.1 Hardware inventory (inc. versions)	OFFICIAL SENSITIVE
A.13 Software Assets	A.13.1 Base software inventory (inc. versions and patch state)	OFFICIAL SENSITIVE
A.14 Locations	A.14.1 Identification of system installation (Site) by Site ID	OFFICIAL
	A.14.2 Identification of system installation at UK site by site or building name	OFFICIAL
	A.14.3 Identification of system installation at overseas sites by site, building name, or unit	OFFICIAL SENSITIVE
A.15 Factory Acceptance Testing	A.15.1 All Factory Acceptance Testing plans and procedures	OFFICIAL SENSITIVE
	A.15.2 Factory Acceptance Testing results and reports	OFFICIAL SENSITIVE
A.16 System Acceptance Testing	A.16.1 Penetration Test reports, Functional testing and security test data which identifies and details system defects, vulnerabilities, and recommendations	OFFICIAL SENSITIVE
	A.16.2 Other system test results and reports from Functional and User testing	OFFICIAL SENSITIVE
A.17 Testing Documentation	A.17.1 All system testing strategies and plans	OFFICIAL SENSITIVE
	A.17.2 Test scripts	OFFICIAL SENSITIVE
	A.17.3 Test results and reports	OFFICIAL SENSITIVE
A.18 Authentication credentials	A.18.1 Details of user accounts and authentication processes (passwords, tokens)	OFFICIAL SENSITIVE
A.19 Cryptographic materials		Up to SECRET
A.20 Live Data		Up to OFFICIAL SENSITIVE
A.21 Personally Identifiable Information	Live Personally Identifiable Information	OFFICIAL-SENSITIVE PERSONAL
	Data Protection Impact Assessment	OFFICIAL SENSITIVE

	Bulk Personal Data Assessment	Up to SECRET
--	-------------------------------	--------------

3. Your attention is drawn to the provisions of the Official Secrets Act 1911-1989 in general, and specifically to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989). In particular you should take all reasonable steps to make sure that all individuals employed on any work in connection with this Contract have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply after completion or earlier termination of the contract
4. Will you please confirm that:
 - a. This definition of the classified aspects of the referenced Contract has been brought to the attention of the person directly responsible for security of classified material.
 - b. The definition is fully understood.
 - c. Measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. [The requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations.]
 - d. All employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this contract.
5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.
6. Classified Information associated with this Contract must not be published or communicated to anyone without the approval of the MOD Contracting Authority.
7. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON
- 76.

Yours faithfully

Copy via email to:

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

Appendix 1
To Security Aspects Letter
Dated:

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: COODSR-IIPCSy@mod.gov.uk).

Definitions

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

Security Grading

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

Security Conditions

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

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material

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

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

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

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

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

8. All UK classified material including documents, media and other assets must be physically secured to prevent unauthorised access. When not in use UK classified material shall be handled with care to prevent 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 35.

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 OFFICIALSENSITIVE 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/HM_G_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 exfiltrate 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 OFFICIALSENSITIVE 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^[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 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 another country for which the UK MOD is responsible.

30. In addition any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD Defence Industry WARP will also advise the Contractor what further action is required to be undertaken.

UK MOD Defence Industry WARP Contact Details

Email: DefenceWARP@mod.gov.uk (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 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.

33. 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 Annex A (MOD Form 1686 (F1686) of ISN 2022/08 is to be used for seeking such approval. The MOD Form 1686 can be found at:

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

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

Physical Destruction

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 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

36. 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;

37. 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-exhibitionclearance-information-sheets>

Publicity Material

38. 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.

39. 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-exhibitionclearance-information-sheets>

Export sales/promotion

40. 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-procedureguidance>

41. 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

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

43. 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

44. 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 – Not Used