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.

1a.	Identification					
	(redacted)					
Call-Off Lot	Lot 2 - Dev, Apps, UX, Dev Ops, Sys Design & Support					
Call-Off Reference	RM6249/DIPS(2)033		Version Number	1.0	Date	12 June 2024
Business Case Reference	Original FBC Number	BC-17997, with funding approved via FCR 23JJ0722A_F				
	Amendment FBC Number	Not Applicable				
Project / equipment for which Services are in support	DevSecOps		Urgent Capability Requirement (UCR)		N/A	
Call-Off Contract title:	BMfS DevSecOps Team Continuation					
Call-Off Contract description:	The BMfS programme is seeking external support to deliver the following non-exhaustive outcomes: • a Common User Platform (CUP) to provide a one-stop shop for support customer to access all relevant information for them to undertake their support request. • Low code applications based on requirements that are outputs of discovery work that will be undertaken. • Support and improvement of the D2S environment being used by BMfS. • Subsequent prioritised work relating to software development or technology.					

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

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)

1b.	Contact details		
Government Directorate / Organisation Title	Defence Digital	Name of Supplier	*PA Consulting Services Ltd - (Prime)*
Name of Requirement Holder's Authorised Representative	███████████	Name of Supplier's Authorised Representative	███████████
Post title	███████████	Post title	███████████
Requirement Holder's Address	Cedar 2A, NH3, Ministry of Defence, Abbey Wood, Stoke Gifford, Bristol BS348JH Stoke Gifford, Bristol	Supplier Address	*10 Bressenden Place, London, SW1E 5DN, United Kingdom*
Postcode	BS34 8JH	Postcode	
Telephone	███████████	Telephone	███████████
Email	███████████	Email	███████████
Unit Identification Number (UIN)		Value Added Tax (VAT) Code	
Resource Accounting Code (RAC)			
Name of Requirement Holder's Project Lead	███████████		
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	03/06/2024	Deadline for Requirement Holder's receipt of Supplier's Call-Off Tender	*11/06/2024*

1c. Statement of Requirements (SOR) (This section 1c. to be completed in full OR a complete SOR to be attached in Appendix 3 of this document)

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

Unique Order Number (defined by delivery team)	FA116		
SOR version issue number	V1.0	SOR dated	03/06/2024
SOR title	20240603 Statement of Work for BMfS Tech and Eng Resources v1.0		

Background/justification for Call-Off Contract
The current BMfS DevSecOps contract expires on 13th June 2024 and due to lack of time and need to retain the services of the incumbent for continuity the Authority is seeking to place a 4-month DIPS direct award to PA Consulting (with Accenture as the Applicant supplier) via Lot 2. This will enable the BMfS project team to use the 4 months to run a competition via DIPS Lot 2 to select a long-term supplier.

Description of Services to be provided under the Call-Off Contract
Please see SOR attached in Appendix 3

Activities required to be undertaken under the Call-Off Contract
Please see SOR attached in Appendix 3

Outputs to be provided under the Call-Off Contract
Please see SOR attached in Appendix 3

Acceptance/rejection criteria / provisions
Please see SOR attached in Appendix 3

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
N/A

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

Critical Service Level Failure
N/A

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

List all Requirement Holder Assets applicable to the Services that shall be issued to the Supplier and returned to the Requirement Holder at termination of the Call-Off Contract
Buyer to provide laptops for access to Virtual MODNET to enable the continued delivery of the service.

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

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

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

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

Project and risk management

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

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

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

Call-Off Start Date	17 June 2024
Call-Off Initial Period	16 weeks
Call-Off Expiry Date	04 October 2024
Call-Off Optional Extension Period	1 month
Minimum notice period prior to a Call-Off Optional Extension Period	2 weeks

SOR approved by (Name in capital letters)		Telephone	
Directorate / Division		Email	
Organisation Role / Position		Date	
Approver's signature			

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

Original FBC Number (*when known*)	Amendment FBC Number (*if applicable*)
BC-17997, with funding approved via FCR 23JJ0722A_F	N/A

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

1d.	Key Deliverables Template

Full details are contained within the Statement of Requirement (SOR) - see Appendix 3

Task Number	Description of Services to be provided	Activities required to be undertaken	Outputs to be provided	Acceptance/rejection criteria / provisions	Milestone Delivery Timeframe
1	**Stock Availability Service**	Develop a service (beta) to enable Front Line Command personnel to check stock availability through the Defence Support Hub that is tailored to the needs of users, ensuring it is intuitive, accessible and aligns with MOD designs and the [GOV.UK](http://gov.uk/) Service Standard.	Achieving a stable secure connection to stock availability data to support delivery of the Stock Availability service. Areas this could cover but not limited to: • providing stock level visibility • improving access to data required to query stock levels, e.g., ESP number, NATO stock number. • where necessary identifying alternative solutions or data sources that can circumvent constraints in data access Development of a stock availability service offering which addresses key Front Line Command user pain points as identified by User Research that support user needs aligned to programme benefits through. • Develop prototypes, wireframes and working examples to support development of the	Authority sign-off and approval of: Technical design and prototype of the stock availability MVP, using the recommendations from the Alpha phase as determined by the discovery outcomes and completed design/technical/solution experimentations.	*[REDACTED]*

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

			service addressing key user pain points in line with User Research • Working with the design team to test the engineering outputs, with users, and work on feedback of the findings to support iteration of the service		

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

| 2 | Development of the Common User Platform | Integrating new services in line with BMfS programme strategy and pipeline priorities including, but not limited to

• Integration of the Check Stock Availability service in Defence Support Hub
• Integration of further services as agreed between Foundry, Defence Digital and the BMfS programme. | Enabling further capabilities in line with the BMfS programme pipeline. Indicative examples of capabilities including, but not limited to

1.1.   Service management approach for services available through the CUP to strategic service management tool (OSM)

1.2.   Support work with the Hybrid Integration Platform (HIP) to ensure a joined-up approach across CUP and HIP.*
Integration of Check Stock Availability Service into CUP
• Develop prototypes, wireframes and working examples to support Stock Availability Service being available via Defence Support Hub.
• Working with the design team to test the engineering outputs, with users, and work on feedback of the findings to support iteration of the Defence Support Hub.
Support of prioritisation of additional services and capabilities being made | Integration of Check Stock Availability Service into CUP completed.
Support prioritisation of additional services and capabilities being made available through the Common User Platform subject to agreement and sign off with Foundry, Defence Digital and the BMfS programme. | [REDACTED] |
| | | | available through the Common User Platform subject to agreement with Foundry, Defence Digital and the BMfS programme. | | |

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

| 3 | **Development of the Hybrid Integration Platform** | Evaluation of BMfS programme recommended integration platform COTS products, and suitability to achieve selected MVP goals. | Design and implement services needed to deploy an MVP Hybrid Integration Platform in line with the strategy and priorities set by the BMfS programme including, but not limited to:

1.3.   Developed as Infrastructure as Code adhering to Secure by Design requirements.

1.4.   Aligned Test Strategy, including approach to environment.

1.5.   Defined release and service management approach to be implemented subsequently.

Investigate feasibility of recommended integration platform COTS products. Develop reusable services using Infrastructure as Code to be deployed into MOD Cloud.
Continuous improvement of HIP MVP to include use cases prioritised by the BMfS programme.*
Advise on BMfS Programme Test Strategy which incorporates HIP.* | Investigate, design and develop a solution to validate the Hybrid Integration Platform MVP, as prioritised and signed off by the BMfS Programme.

Support prioritisation of additional use cases and capabilities to be made available through the Hybrid Integration Platform subject to agreement and sign off with Foundry, Defence Digital and the BMfS programme. | [REDACTED] |

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

2.	Call-Off Incorporated Terms

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

1   This Order Form including the General Conditions in section 2(b) and the Call-Off Special Terms in section 2(c).

2   Joint Schedule 1 (Definitions)

3   Any Statement(s) of Work (in the form of the template set out in Appendix 4 to this Framework Schedule 6 (Order Form Template, Statement of Requirements Template)) executed by the Requirement Holder and the Supplier with a corresponding Call-Off Contract reference

4   [Framework Special Terms] No special terms included.

5   The following Schedules in equal order of precedence:

- Joint Schedules ○   Joint Schedule 2 (Variation Form) ○   Joint Schedule 3 (Insurance Requirements) ○   Joint Schedule 4 (Commercially Sensitive Information) ○   Joint Schedule 5 (Corporate Social Responsibility) ○   Joint Schedule 10 (Rectification Plan) ○   Joint Schedule 11 (Processing Data)

- Call-Off Schedules ○   Call-Off Schedule 2 (Staff Transfer), Parts A, B, C [**A, B and C Optional – see guidance note within Call-Off Schedule 2**] and D.
   - ○   Call-Off Schedule 3 (Continuous Improvement) ○   Call-Off Schedule 5 (Pricing Details and Expenses Policy) ○   Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) ○   Call-Off Schedule 8 (Business Continuity and Disaster Recovery) ○ Call-Off Schedule 9 (Security) ○   Call-Off Schedule 10 (Exit Management)
   - ○   Call-Off Schedule 13 (Implementation Plan and Testing) ○   Call-Off Schedule 14 (Service Levels) ○   Call-Off Schedule 17 (MOD Terms) ○   Call-Off Schedule 25 (Ethical Walls Agreement) ○   Call-Off Schedule 26 (Cyber)

6   Core Terms (DIPS version)

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

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

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)	Direct award		
Direct award	☒				
		Weighting (Technical)	N/A	Weighting (Price)	N/A

2b.	General Conditions	
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. The Supplier confirms all members of the team proposed are on the Supplier's payroll and therefore are subject to PAYE. • Within the scope of the Call-Off Contract, the Supplier will provide individuals holding current SC security clearance; evidence of which is be provided prior to the start date.		☒

2c.	Call-Off Special Terms
The following Special Terms are incorporated into this Call-Off Contract:	
None.	

2d.	Call-Off Charges	
Capped Time and Materials (CTM)		☐
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		☒

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

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

Reimbursable Expenses

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

2e.	Payment Method
Requirement Holder's Invoice Address **Requirement Holder's Authorised Representative**	

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

2f. Milestone Payments Schedule (MPS) (expand table as appropriate)				13
Milestone/ Stage Payment number	**Key Deliverable**	**Due Date**	**%**	**Milestone Payment**
				value £ (ex VAT)
1	Stock Availability Service			
2	Development of Common User Platform - July			
3	Development of Common User Platform – August			
4	Development of Hybrid Integration Platform - September			
5	Development of Hybrid Integration Platform - October			
6				
7				
8				
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		**£896,523.00**

The Authority should note that the budget is not sufficient for all activities outlined within the SOR the Supplier will work with the Authority to prioritise as much as Deliverable 3 as is possible within the timescales, noting a reprioritisation activity is currently happening.

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

2g.	Maximum Liability

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

2h.	Requirement Holder's Environmental Policy

Available online at: Management of environmental protection in defence (JSP 418) - GOV.UK (www.gov.uk)

This version is dated 18th August 2023.

2i.	Requirement Holder's Security Policy

Security Aspects Letter has been issued and executed alongside this Order Form. See Appendix 6.

2j.	Progress Reports and meetings		
Progress Report Frequency	**Monthly**	Progress Meeting Frequency	Monthly

2k.	*Quality Assurance Conditions*	
According to the product or scope of the work to be carried out, the Supplier shall meet the following requirements:		
Allied Quality Assurance Publications (AQAP) 2110 – North Atlantic Treaty Organization (NATO) Quality Assurance Requirements for Design, Development and Production. 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	☒

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

2l.	Key Staff

2m.	Key Subcontractor(s)

2n.	Commercially Sensitive Information

- All supplier financial information
- Supplier team structure and information relating to individuals

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 plan already in existence	☐

3.	Charges
Estimated Contract Value (excluding VAT) for Call-Off Contract	

4.	Additional Insurances

Not Applicable

5.	Guarantee
Not Applicable	

6.	Social Value Commitment
Not Applicable	

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

7.	Requirement Holder Commercial Officer Authorisation		
Order Form approved by (Name in capital letters)		Telephone	
Directorate / Division		Email	
Organisation Role / Position		Date	
Approver's signature			

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

9.	Final Administration
On receipt of the Order Form acknowledgement from the Supplier, the Commercial Manager (who placed the order) **must** send an electronic copy of the acknowledged Order Form, together with any applicable Appendix 3 to this Schedule 6, directly to *DIPS Professional Services Team* at the following email address:	

Appendix 1 - Addresses and Other Information

1. Commercial Officer
Name: ███████████████

Address:
███████████████

Email: ███████████████

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

Address: ███████████████

Email: ███████████████

3. Packaging Design Authority Organisation & point of contact:
N/A

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

☐

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

☐

   (b) U.I.N.

5. Drawings/Specifications are available from
N/A

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

2.   For all other enquiries contact DES Fin FA-AMET
Policy, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
☐

9. Consignment Instructions
The items are to be consigned as follows:

10. Transport. The appropriate Ministry of Defence Transport Offices are:
A. DSCOM, DE&S, DSCOM, MoD Abbey Wood, Cedar 3c, Mail Point 3351, BRISTOL BS34 8JH
Air Freight Centre
Surface Freight Centre

B. JSCS

JSCS Helpdesk No
JSCS Fax No.
Users requiring an account to use the MOD Freight Collection Service should contact in the first instance.

11. The Invoice Paying Authority
      Website is:
https://www.gov.uk/government/organisations/ministryof-defence/about/procurement

6. Intentionally Blank	12. Forms and Documentation are available through *: Ministry of Defence, Forms and Pubs Commodity Management PO Box 2, Building C16, C Site Lower Arncott Bicester, OX25 1LP **Applications via fax or email:**

7. Quality Assurance Representative:	* NOTE 1. Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Internet Site:
Commercial staff are reminded that all Quality Assurance requirements should be listed under the General Contract Conditions. **AQAPS** and **DEF STANs** are available from UK Defence Standardization, for access to the documents and details of the helpdesk visit http://dstan.gateway.isgr.r.mil.uk/index.html [intranet] or https://www.dstan.mod.uk/ [extranet, registration needed].	https://www.kid.mod.uk/maincontent/business/commercial/index.htm 2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.

Appendix 1 to Schedule 6

14

Appendix 2 – Supplier's Quotation - Charges Summary

Supplier Charges summary: To be completed by the Supplier in support of a quotation provided in response to an ITT for the requirement captured on the above Order Form.   *NOT USED – Supplier Cover Letter and Excel provided*

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 ▐▐▐▐▐▐▐			
	Meals ▐▐▐▐			
	Miscellaneous costs (please define below)			
		The above T&S costs relate to the period to		

Subcontractor price

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 Requirements Template)
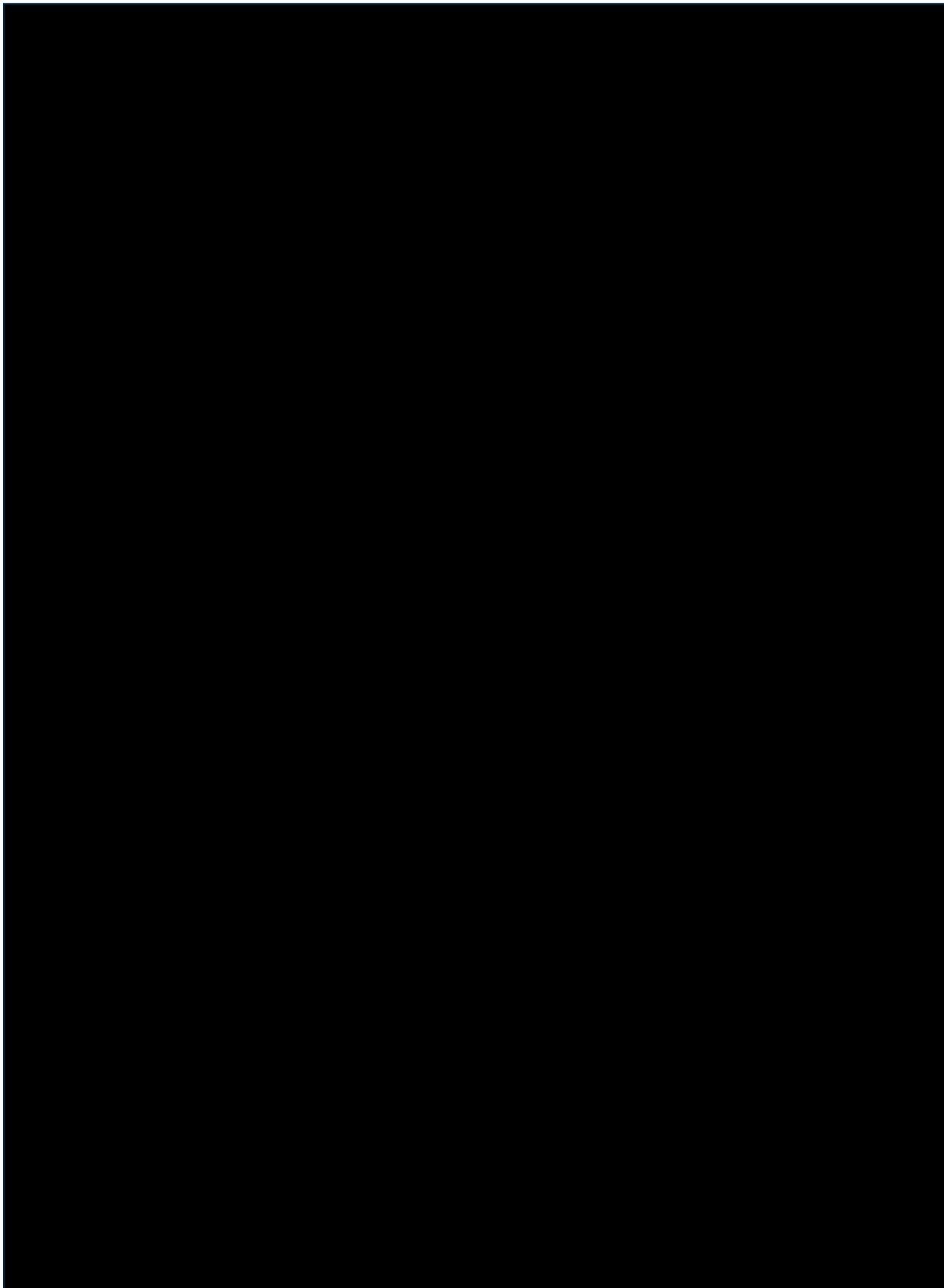
Appendix 3

Appendix 4 (Template Statement of Work)

[Requirement Holder Guidance: This is a template Statement of Work for use when required as part of a Call-Off Contract Order Form. This is likely to be useful for projects with multiple separate requirements. Any SOW which has been completed prior to execution of the Order Form should be attached to Appendix 3 of the Order Form]

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

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

[**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)]

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

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)
Annex 1 to Statement of Work

Data Processing - <mark>N/A</mark>

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

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** 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: ● [**Insert** the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority] **The Supplier is Controller and the Relevant Authority is Processor** 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: ● [**Insert** the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier] **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: ● [**Insert** the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together] **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: ● Business contact details of Supplier Personnel for which the Supplier is the Controller, ● Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller, ● [**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]

	[**Guidance** where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship
	identified]
Duration of the Processing	[Clearly set out the duration of the Processing including dates]

Nature and purposes of the Processing	[Be as specific as possible, but make sure that you cover all intended purposes.
	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.
	The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]
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.

OFFICIAL SENSITIVE (when complete)

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

Strategic Command
Mustang Building, MOD Corsham,
Westwells Road,
CORSHAM, SN13 9NR

Chief Information Security Officer

Date of Issue: 11th June 2024

For the attention of:
Tom Birch
PA Consulting Services Ltd

Defence DevSecOps (D2S)

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 outlines the minimum measures required to safeguard OFFICIAL and SECRET assets and information.

Aspects	Classification
For D2S services operating at OFFICIAL classification (inclu ing handling aveats)	
Existence of project and in-service date	OFFICIAL

Highest classification of information to be stored and processed	OFFICIAL with a handling caveat of SENSITIVE
Location and details (including names) of services and users	OFFICIAL with a handling caveat of SENSITIVE
High level architecture providing a nondetailed view of the system/service	OFFICIAL
Low level Architecture documentation and diagrams which contains details pertaining to the hosting and configuration of the system	OFFICIAL with a handling caveat of SENSITIVE
Complete set of design documentation (LLD/HLD)	OFFICIAL with a handling caveat of SENSITIVE
User data (name, organisation, contact	OFFICIAL with a handling caveat of

details) for all users	SENSITIVE
Secure by Design assurance collateral documentation i.e., Self-Assessment, Risk Assessment, IT Health Check etc	OFFICIAL with a handling caveat of SENSITIVE
Supplier Assurance Questionnaire responses (all data fields)	OFFICIAL with a handling caveat of SENSITIVE
Logs and details of helpdesk correspondence	OFFICIAL or; OFFICIAL with SENSITIVE a handling caveat of
Login credentials for normal and privileged users	OFFICIAL with a handling caveat of SENSITIVE
Physical security of assets such as servers, infrastructure et al, stored in supplier premises	OFFICIAL with a handling caveat SENSITIVE of
Details of Cloud Hosting provider, excluding designs, routing, configuration information	OFFICIAL
Details of Cloud Hosting provider, including designs, routing, configuration information	OFFICIAL with a handling caveat of SENSITIVE
A single IP address with no context or connection to the service	OFFICIAL
Aggregation of multiple IP addresses with or without context to the system	OFFICIAL with a handling caveat of SENSITIVE
Complete set of IP addresses	OFFICIAL with a handling caveat of SENSITIVE
Obfuscated DNS/hostname information pertaining to the system, or DNS information without context to the system	OFFICIAL
Full DNS/hostname information, with context to the system	OFFICIAL with a handling caveat of SENSITIVE
User Requirements Documentation	OFFICIAL

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

Requirements generated from user community engagement without operational context	OFFICIAL
Requirements generated from user community engagement with operational context	OFFICIAL with a handling caveat of SENSITIVE
Details of 3rd party software components that make up the system	OFFICIAL, or; OFFICIAL with a handling caveat of SENSITIVE
Risk Management Documentation	OFFICIAL with a handling caveat of SENSITIVE
Information pertaining to Penetration Testing or detailed vulnerabilities of the system	OFFICIAL with a handling caveat of SENSITIVE ndlir Only
File Type Control Policy, including 'dirty word' list	OFFICIAL with a handling caveat of SENSITIVE

Project management information, including management plans, financial details, programme status, supply chain information (excluding risk artefacts).	OFFICIAL, or; OFFICIAL with a handling caveat of SENSITIVE
Project contracts (not in the public domain), contracts and/or agreements relating to third parties and the wider supply chain	OFFICIAL with a caveat of handling SENSITIVE (Commercial)
Software inventory with insufficient detail to provide an overview of the system, risk or whole-system context	OFFICIAL
Software inventory including patching, version information, vulnerabilities, CVEs, protection information or policies relating to usage	OFFICIAL with a handling caveat of SENSITIVE
Complete system/network installation and configuration documentation	OFFICIAL with a handling caveat of SENSITIVE
Aggregated system/network installation, guidance, usage notes, user guides and/or configuration information	OFFICIAL, or; OFFICIAL with a handling caveat of SENSITIVE
Detailed information relating to users of the system, including sites, purpose, roles and personally identifiable information	OFFICIAL OFFICIAL with a handling caveat of SENSITIVE (Personal)

Functional testing and/or system testing reports, including statistical reporting of testing progress. Also includes system acceptance testing	OFFICIAL, or; OFFICIAL with a handling caveat of SENSITIVE
Operational data, including test data that could be misconstrued as operation data	OFFICIAL with a handling caveat of SENSITIVE
Passwords, pins or other login and authentication data. Information relating to password storage, algorithms, policies, etc.	OFFICIAL with a handling caveat of SENSITIVE
Cryptographic material	N/A
All aspects of service management, including overview, process, account management, working instructions, user guides	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
Details relating to Security Operations Centre, including location, management, instructions, data transfer, operational usage, procedural or technical information	OFFICIAL with a handling caveat of SENSITIVE
FAQs, training material, usage guides, installation instructions, community user guides (including those of COTS/MOTS components)	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
Details of the applications residing within the system environments (applications and data of onboarded teams)	OFFICIAL or;

	OFFICIAL with a handling caveat of SENSITIVE
Business Continuity and Disaster Recovery Plans, including plans to exercise the BCDR	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
The operation of tooling within the system, it's purpose and operation as well as data held within the tooling	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
Repositories that are protected from public view (e.g. by way of MOD access management)	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE

Any information that has been endorsed for public disclosure, including system information, source code, repositories, user guides, system context, e.t.c	OFFICIAL
For services operating at SECRET classification (including handling caveats)	
Existence of project and in-service date	OFFICIAL
Highest classification of information to be stored and processed	SECRET with additional handling caveats
Location and details (including names) of services and users	OFFICIAL with a handling caveat of SENSITIVE
High level architecture providing a non-detailed view of the system/service	SECRET with a handling caveat of UK EYES ONLY
Low level Architecture documentation and diagrams which contains details pertaining to the hosting and configuration of the system	OFFICIAL with a handling caveat of SENSITIVE
Complete set of design documentation (LLD/HLD)	SECRET with a handling caveat of UK EYES ONLY
User data (name, organisation, contact details) for all users	OFFICIAL with a handling caveat of SENSITIVE
Secure by Design assurance collateral documentation i.e. Self Assessment, Risk Assessment, IT Health Check etc	OFFICIAL with a handling caveat of SENSITIVE or; SECRET with a handling caveat of UK EYES ONLY
Supplier Assurance Questionnaire responses (all data fields)	OFFICIAL with a handling caveat of SENSITIVE
Logs and details of helpdesk correspondence	OFFICIAL with a handling caveat of

	SENSITIVE
Login credentials for normal and privileged users	SECRET UK EYES ONLY
Physical security of assets such as servers, infrastructure et al, stored in supplier premises	SECRET UK EYES ONLY
Details of Cloud Hosting provider, excluding designs, routing, configuration information	OFFICIAL

OFFICIAL SENSITIVE (when complete)

36

Details of Cloud Hosting provider, including designs, routing, configuration information	OFFICIAL with a handling caveat of SENSITIVE or; SECRET with a handling caveat of UK EYES ONLY
A single IP address with no context or connection to the service	OFFICIAL with a handling caveat of SENSITIVE
Aggregation of multiple IP addresses with or without context to the system	SECRET UK EYES ONLY
Complete set of IP addresses	SECRET UK EYES ONLY
Obfuscated DNS/hostname information pertaining to the system, or DNS information without context to the system	OFFICIAL with a handling caveat of SENSITIVE
Full DNS/hostname information, with context to the system	SECRET UK EYES ONLY
User Requirements Documentation	OFFICIAL with a handling caveat of SENSITIVE
Requirements generated from user community engagement without operational context	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
Requirements generated from user community engagement with operational context	OFFICIAL with a handling caveat of SENSITIVE or; SECRET with a handling caveat of UK EYES ONLY
Details of 3rd party software components that make up the system	OFFICIAL with a handling caveat of SENSITIVE
Risk Management Documentation	SECRET UK EYES ONLY
Information pertaining to Penetration Testing or detailed vulnerabilities of the system	SECRET UK EYES ONLY
File Type Control Policy, including 'dirty word' list	SECRET UK EYES ONLY
Project management information, including management plans, financial details, programme status, supply chain information (excluding risk artefacts).	OFFICIAL, or; OFFICIAL with a handling caveat of

	SENSITIVE

OFFICIAL SENSITIVE (when complete)

37

Project contracts (not in the public domain), contracts and/or agreements relating to third parties and the wider supply chain	OFFICIAL with a handling caveat of SENSITIVE (Commercial)
Software inventory with insufficient detail to provide an overview of the system, risk or whole-system context	OFFICIAL with a handling caveat of SENSITIVE
Software inventory including patching, version information, vulnerabilities, CVEs, protection information or policies relating to usage	SECRET UK EYES ONLY
Complete system/network installation and configuration documentation	SECRET UK EYES ONLY
Aggregated system/network installation, guidance, usage notes, user guides and/or configuration information	OFFICIAL with a handling caveat of SENSITIVE or; SECRET with a handling caveat of UK EYES ONLY
Detailed information relating to users of the system, including sites, purpose, roles and personally identifiable information	OFFICIAL with a handling caveat of SENSITIVE or; SECRET UK EYES ONLY
Functional testing and/or system testing reports, including statistical reporting of testing progress. Also includes system acceptance testing	OFFICIAL with a handling caveat of SENSITIVE
Operational data, including test data that could be misconstrued as operational data	OFFICIAL with a handling caveat of SENSITIVE or; SECRET with a handling caveat of UK EYES ONLY
Passwords, pins or other login and authentication data. Information relating to password storage, algorithms, policies, etc.	SECRET UK EYES ONLY
Cryptographic material	SECRET UK EYES ONLY
All aspects of service management, including overview, process, account management, working instructions, user guides	OFFICIAL with a handling caveat of SENSITIVE

OFFICIAL SENSITIVE (when complete)

Details relating to Security Operations Centre, including location, management, instructions, data transfer, operational usage, procedural or technical information	OFFICIAL with a handling caveat of SENSITIVE or; SECRET with a handling caveat of UK EYES ONLY
FAQs, training material, usage guides, installation instructions, community user guides (including those of COTS/MOTS components)	OFFICIAL or;
	OFFICIAL with a handling caveat of SENSITIVE
Details of the applications residing within the system environments (applications and data of onboarded teams)	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
Business Continuity and Disaster Recovery Plans	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
The operation of tooling within the system, it's purpose and operation as well as data held within the tooling	OFFICIAL with a handling caveat of SENSITIVE
Repositories that are protected from public view (e.g. by way of MOD access management)	OFFICIAL or; OFFICIAL with a handling caveat of SENSITIVE
Any information that has been endorsed for public disclosure, including system information, source code, repositories, user guides, system context, etc.	OFFICIAL

The table below stipulates the roles and responsibilities of key personnel working on the project. This is separated into the respective classifications of each system.

NOTE: Personnel working across multiple classifications must meet the minimum required clearance of the highest classification system.

For example, where a Solution Lead works on both OFFICIAL and SECRET systems, the minimum required clearance would be Security Check. Where a DevOps SME is working solely on OFFICIAL systems, their minimum clearance would be BPSS.

Key Roles related to the design, development and operation of the system(s)		
Role	Description	Minimum Required Clearance
For services operating at OFFICIAL classification (including handling caveats)		

Solution Lead	Overall responsibility for ASH, RedHat and DevSecOps. Designs technical architecture, translates to project tasks and manages team resources and customer requirements	SC
DevOps Lead	Overall responsibility for the design, implementation, documentation and accreditation of the DevOps tools and processes. Responsible for stakeholder engagement, work package	SC

	design and progress reporting. Responsible for assurance, discovery, and architecture design.	
DevOps SME	Responsible for supporting the DevOps Team lead, implementing DevOps tooling, producing documentation, and facilitating progress of the DevOps stream	BPSS
Azure Lead	Overall responsibility for the design, implementation, documentation and accreditation of the ASH including tools and processes. Responsible for stakeholder engagement, work package design and progress reporting. Responsible for assurance, discovery, and architecture design.	SC
Azure SME	Responsible for supporting the Azure Lead, implementing configuration, tooling, producing documentation, and facilitating progress of the ASH stream	BPSS
Redhat Platform Lead	Overall responsibility for the design, implementation, documentation and accreditation of the RedHat platform and processes. Responsible for stakeholder engagement, work package design and progress reporting. Responsible for assurance, discovery, and architecture design.	SC

Redhat SME	Provide all relevant and required technical insights to the project team, making available the technical information required to design, implement, and operate the platform to the team in a timely manner as possible, assisting with configuration as needed. Responsible for review and sign off on solution configuration and documentation. Support the Azure, RedHat and DevOps Leads as necessary	BPSS

Scrum Master	Support the Solution Lead in creating backlogs, identifying, mapping and tracking dependencies, progress, changes to timeframe and all environmental impact to the project (including holidays, illness, planned environment outage etc). Detailed action tracking and progress reporting	BPSS
User Researcher	Responsible for identifying all user needs unique to Foundry DevSecOps.	BPSS
Assignment Manager	Providing overall alignment and execution across all Foundry DevSecOps SOWs, including governance with client.	SC
Security Lead(s)	Responsible for engaging the Security Assurance stream and translating requirements identified into Security Strategy. Responsible for overall strategy for technical security controls across all platform components, responsible for definition of and prioritisation of Security Engineering work packages. Responsible for achieving ATT and IATO for the solution, including Authority engagement and engagement with other project roles as needed	SC

Security Engineering	Responsible for assuring technical security controls are implemented on the platform in accordance with strategy as set by Security Lead, vendor best practice and Secure by Design. Responsible for ensuring that all technical controls are auditable and reportable.	SC
Penetration Testers	Responsible for testing all OFFICIAL services for potential security vulnerabilities, weaknesses, misconfiguration or poor practice, policy and procedure. To report vulnerabilities back through the relevant teams.	SC

Service Management Personnel (no privileged access)	Responsible for providing a full-service management solution, including account management, live support, user guidance and system monitoring.	BPSS
Service Management Personnel (with privileged access)	Responsible for providing a full-service management solution, including account management, live support, user guidance and system monitoring. Users will have full administrative rights across the system.	SC
For services operating at SECRET classification (including handling caveats)		
Solution Lead	Overall responsibility for ASH, RedHat and DevSecOps. Designs technical architecture, translates to project tasks and manages team resources and customer requirements	SC Sole UK National
DevOps Lead	Overall responsibility for the design, implementation, documentation and accreditation of the DevOps tools and processes. Responsible for stakeholder engagement, work package design and progress reporting. Responsible for assurance, discovery, and architecture design.	SC Sole UK National

DevOps SME	Responsible for supporting the DevOps Team lead, implementing DevOps tooling, producing documentation, and facilitating progress of the DevOps stream	SC Sole UK National
Azure Lead	Overall responsibility for the design, implementation, documentation and accreditation of the ASH including tools and processes. Responsible for stakeholder engagement, work package design and progress reporting. Responsible for assurance, discovery, and architecture design.	SC Sole UK National
Azure SME	Responsible for supporting the Azure Lead, implementing configuration, tooling,	SC Sole UK National

	producing documentation, and facilitating progress of the ASH stream	
Redhat Platform Lead	Overall responsibility for the design, implementation, documentation and accreditation of the RedHat platform and processes. Responsible for stakeholder engagement, work package design and progress reporting. Responsible for assurance, discovery, and architecture design.	SC Sole UK National
Redhat SME	Provide all relevant and required technical insights to the project team, making available the technical information required to design, implement, and operate the platform to the team in a timely manner as possible, assisting with configuration as needed. Responsible for review and sign off on solution configuration and documentation. Support the Azure, RedHat and DevOps Leads as necessary	SC Sole UK National

Scrum Master	Support the Solution Lead in creating backlogs, identifying, mapping and tracking dependencies, progress, changes to timeframe and all environmental impact to the project (including holidays, illness, planned environment outage etc). Detailed action tracking and progress reporting	BPSS – No regular access to information above OFFICIAL
User Researcher	Responsible for identifying all user needs unique to Foundry DevSecOps.	BPSS – No regular access to information above OFFICIAL
Assignment Manager	Providing overall alignment and execution across all Foundry DevSecOps SOWs, including governance with client.	SC Sole UK National
Security Lead(s)	Responsible for engaging the Security Assurance stream and translating requirements identified into Security Strategy. Responsible for overall strategy for technical	SC Sole UK National
	security controls across all platform components, responsible for definition of and prioritisation of Security Engineering work packages. Responsible for achieving ATT and IATO for the solution, including Authority engagement and engagement with other project roles as needed	
Security Engineering	Responsible for assuring technical security controls are implemented on the platform in accordance with strategy as set by Security Lead, vendor best practice and Secure by Design. Responsible for ensuring that all technical controls are auditable and reportable.	SC Sole UK National

Penetration Testers	Responsible for testing all SECRET services for potential security vulnerabilities, weaknesses, misconfiguration or poor practice, policy and procedure. To report vulnerabilities back through the relevant teams.	Developed Vetting
Service Management Personnel (no privileged access)	Responsible for providing a full-service management solution, including account management, live support, user guidance and system monitoring.	SC Sole UK National
Service Management Personnel (with privileged access)	Responsible for providing a full-service management solution, including account management, live support, user guidance and system monitoring. Users will have full administrative rights across the system.	Developed Vetting or; SC with Developed Vetting in progress

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.

OFFICIAL SENSITIVE (when complete)

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.

8.   If you believe that the classification of the aspects has materially increased from the level described herein, please contact the MOD Project Officer immediately to discuss, arrange and agree if any additional security controls for communication of such material are required.

Yours faithfully

Copy via email to: [REDACTED]