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

**Order Form**

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

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

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

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

| **1a. Identification** | | | | | |
|---|---|---|---|---|---|
| Call-Off Lot | Lot 3 | | | | |
| Call-Off Reference | RM6249/DIPS(03)025 | Version Number | 1.0 | Date | 29/05/2024 |
| Business Case Reference | Original FBC Number | DD-FI-DDPT- Digital Policy Project | | | |
| | Amendment FBC Number | DD-FI-DDPT- Digital Policy Project | | | |

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

| | | | |
|---|---|---|---|
| Project / equipment for which Services are in support | Provision of cyber, technology and data Professional Services support | Urgent Capability Requirement (UCR) | N/a |

| | |
|---|---|
| Call-Off Contract title: | PS439 Digital Policy Service |
| Call-Off Contract description: | Professional services support is required to retire and replace JSP604 with a holistic set of Digital Policy, achieving required outcomes. |

**1b. Contact details**

| | | | |
|---|---|---|---|
| Government Directorate / Organisation Title | Defence Digital, Strategic Command | Name of Supplier | *PA Consulting Services Ltd - (Prime)* |
| Name of Requirement Holder's Authorised Representative | [redacted] | Name of Supplier's Authorised Representative | [redacted] |
| Post title | [redacted] | Post title | [redacted] |
| Requirement Holder's Address | Spur B3, Building 405, MOD Corsham, Wiltshire SN13 9NR | Supplier Address | 10 Bressenden Place, London, SW1E 5DN, United Kingdom |
| Postcode | | Postcode | |
| Telephone | [redacted] | Telephone | [redacted] |
| Email | [redacted] | Email | [redacted] |
| Unit Identification Number (UIN) | D2412A | Value Added Tax (VAT) Code | GB 238 5350 57 |
| Resource Accounting Code (RAC) | NPB026 | | |
| Name of Requirement Holder's Project Lead | | | |

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

| | | | |
|---|---|---|---|
| Requirement Holder's Secondary Contact Name | [redacted] | Supplier Secondary Contact Name | [redacted] |
| Requirement Holder's Secondary Contact Role | [redacted] | Supplier Secondary Contact Role | [redacted] |
| Requirement Holder's Secondary Contact Email | [redacted] | Supplier Secondary Contact Email | [redacted] |

| | | | |
|---|---|---|---|
| **Date that the Statement of Requirements was issued** | 13/05/2025 | **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 7 of this document)**

| | | | |
|---|---|---|---|
| Unique Order Number (defined by delivery team) | DD-FI-DDPT- Digital Policy Project | | |
| SOR version issue number | 1 | SOR dated | 28/05/2024 |
| SOR title | Digital Policy Transformation Statement of Work | | |

| |
|---|
| Background/justification for Call-Off Contract |

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

The Digital Policy Service is comprised of a number of change elements; Digital Policy Transformation and Cabinet Office Digital and Technical (D&T) Spend Controls which when combined, aim to deliver against Defence Digital Strategic Objective 6 (SO6)1.

With the CIOs strategic intent to radically transform Digital Policy and Standards, changing the way users' access and interact with them, this Policy Project builds on previous discovery project work. This will enable the retirement and replacement of JSP604 The Defence Manual of ICT policy and standards by September 2024.

The authority seeks to place a **direct award** contract through DIPS Lot 3 (Cyber Security, Crypto, Sec Ops & Integrated Systems) for Professional Services for 5 months, from June 2024 to October 2024. This is required to bring in skilled and experienced staff to retire and replace JSP604 with a holistic set of Digital Policies, achieving required outcomes.

The scope for Phase 2 – 4 (June 2024 – October 2024) will focus on JSP 604 Rule fit. This follows the completion of Phase 1 (Feb 2024 – March 2024) under an earlier DIPS Direct Award contract with PA Consulting with Accenture as secondary supplier (PS 359). Wider artefacts will be included as Digital Allies team and as MOD capacity and engagement allows.

The Contract is for 5 months (June 2024 to October 2024) at a cost of £625,000.00 exc VAT.

This Direct Award is to conclude the urgent policy revisions work already underway and ensure continuity with the current supplier, Accenture. Any further policy work will be competed through DIPS.

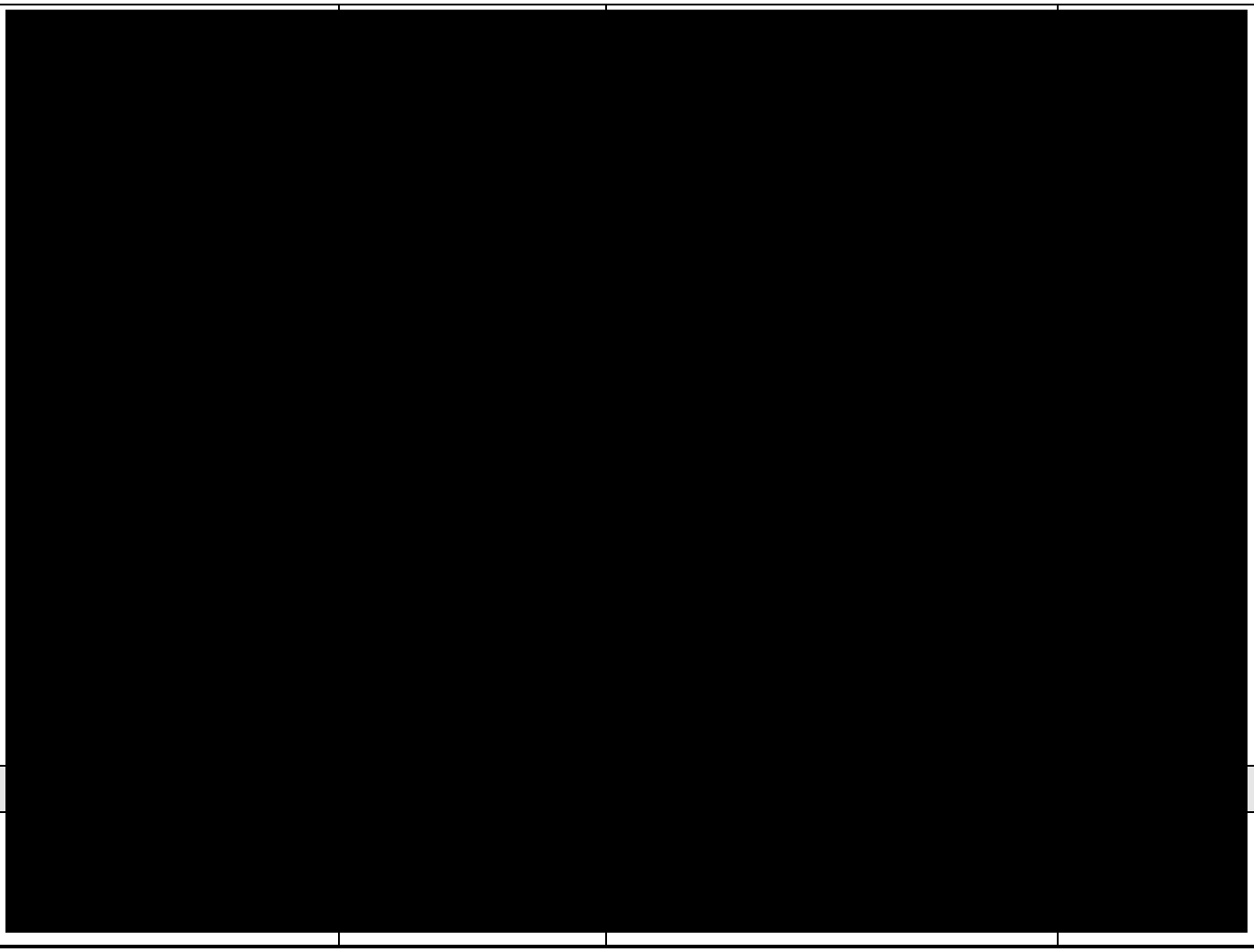
Description of Services to be provided under the Call-Off Contract

The provision of cyber, technology and data Professional Services support to complete JSP 604 Digital Policy work and deliver required outcomes.

Activities required to be undertaken under the Call-Off Contract

| Requirement | Outcome(s) | Deliverable | Date due |
|---|---|---|---|
| **Phase 2 – Mobilisation and re-baseline (1 month)** | | | |

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



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

[redacted]

| **Phase 4 – MVP Implementation (4 weeks)** |
| --- |
| [redacted] |
| Outputs to be provided under the Call-Off Contract |
| See Table above - “Activities required to be undertaken under the Call-Off Contract” – Outcomes. Both phases of the Costed Option 1 must be enacted together. |
| Acceptance/rejection criteria / provisions |

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

See Table above - “Activities required to be undertaken under the Call-Off Contract” – Deliverables.

Acceptance of the deliverables will be provided by the Authority when the deliverables materially conform to the descriptions outlined above.
The deliverables will be reviewed in line with the following review process:

- Following submission of the Deliverables to the Authority, it has 3 Working Days to provide comments or approval to the Supplier.
- Following receipt of the comments, the Supplier has 2 Working Days to respond to the Authority upon return of the comments.
- Following responses to the above, the Authority has 1 Working Day to respond and provide approval or further comments. Where further comments are provided the Customer and Supplier will jointly agree the timelines for resolution.

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** |
|---|
| Delivery of Deliverables by specific date as specified in the Table above - “Activities required to be undertaken under the Call-Off Contract”<br>Measurement: Deliverables to be delivered on time<br>Red: 5 days late<br>Amber: 1-4 day late<br>Green: on time |
| |

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

| **Critical Service Level Failure** |
|---|
| Not applicable |
| |

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

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

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

Due to level of data and information/artefact development a MOD Laptop to be provided, if unavailable MOD virtual desktop to be provided as an interim measure.

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

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

- No specific Quality Management System requirements are defined. This does not relieve the Supplier of providing conforming products under this contract. 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

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.

[redacted]

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

| | |
|---|---|
| Call-Off Start Date | 11/06/2024 |
| Call-Off Initial Period | 5 Months |
| Call-Off Expiry Date | 11/11/2024 |
| Call-Off Optional Extension Period | N/A |

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

| | |
|---|---|
| Minimum notice period prior to a Call-Off Optional Extension Period | N/A |

| | | | |
|---|---|---|---|
| SOR approved by (Name in capital letters) | [redacted] | Telephone | [redacted] |
| Directorate / Division | [redacted] | Email | [redacted] |
| Organisation Role / Position | [redacted] | Date | 31/01/2024 |
| Approver's signature | [redacted] | | |

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

| **Original FBC Number** (*when known*) | **Amendment FBC Number** (*if applicable*) |
|---|---|
| DD-FI-DDPT- Digital Policy Project | n/a |

**1d. Key Deliverables Template**

*Brief summary of the requirement – expand/delete rows as appropriate. Full details appear below or are contained within the Statement of Requirement (SOR)*

| **Requirement** | **Outcome(s)** | **Deliverable** | **Date due** |
|---|---|---|---|
| [redacted] | | | |

# DIPS Order Form / Statement of Requirements Template

# (Framework Schedule 6)

## 2. Call-Off Incorporated Terms

# 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] [**Requirement Holder guidance:** This will incorporate all of the Framework Special Terms into the Call-Off Contract. This will need to be amended to specify which are included if it is anticipated that some will be excluded]

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) **Part A** ○ 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 | ☒**Error! Bookmark not defined.** | | | | |
| | | 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:<br><br>*Additional Conditions:*<br>• *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.*<br>• *SC clearance required as a minimum.* | ☒ |

| 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 | |
| Monthly payments in arrears to be paid against deliverables<br>No T&S is available<br><br>**Reimbursable Expenses**<br><br>[None] | |

| 2e. Payment Method |
|---|

# DIPS Order Form / Statement of Requirements Template

## (Framework Schedule 6)

CP&F monthly payment in arrears
PO Number TBC

**Requirement Holder's Invoice Address**

[redacted]

**Requirement Holder's Authorised Representative**

[redacted]

Strategic Command,
Defence Digital
Spur C3, Building 405,
MOD Corsham, Westwells Roa
Corsham,
Wilts SN13 9NR

Milestones to be reviewed prior to contract extension.

# DIPS Order Form / Statement of Requirements Template

## (Framework Schedule 6)

| | Milestone/ Stage Payment number | Key Deliverable | Due Date | % | Milestone Payment value £ (ex VAT) |
|---|---|---|---|---|---|
| Phase 2 | 2.1 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 2.2 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 2.4 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 2.4 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 2.5 | [redacted] | [redacted] | [redacted] | [redacted] |
| Phase 3 | 3.1 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.2 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.3 | [redacted] | [redacted] | [redacted] | [redacted] |

# DIPS Order Form / Statement of Requirements Template

## (Framework Schedule 6)

| | | | | | |
|---|---|---|---|---|---|
| | 3.4 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.5 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.2 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.6 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.7 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.8 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 3.9 | [redacted] | [redacted] | [redacted] | [redacted] |
| Phase 4 | 4.1 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 4.2 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 4.3 | [redacted] | [redacted] | [redacted] | [redacted] |
| | 4.4 | [redacted] | [redacted] | [redacted] | [redacted] |
| | **FINAL Payment** | [redacted] | [redacted] | [redacted] | [redacted] |
| | | | **Total Contract Value** | | **£625,000** |

# 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)<br><br>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 | **Fortnightly & Monthly** | Progress Meeting Frequency | **Fortnightly & 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.<br><br>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 | X☒ |
| 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** |
|---|
| N/A |

| **2m. Key Subcontractor(s)** |
|---|
| [redacted] |

| **2n. Commercially Sensitive Information** |
|---|
| Supplier 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 CallOff Schedule 26 (Cyber). | RAR-240410A11 Risk Profile: N/A |

| 2p. Implementation Plan | |
|---|---|
| Not applicable | ☐ |

| 3. Charges |
|---|
| Estimated Contract Value (excluding VAT) for Call-Off Contract |
| £625,000.00 exc VAT |

| 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) | [redacted] | Telephone | [redacted] |
| Directorate / Division | [redacted] | Email | [redacted] |
| Organisation Role / Position | [redacted] | Date | 11 June 2024 |

| | |
|---|---|
| Approver's signature | [redacted] |

## 8. Acknowledgement by Supplier

| | | | |
|---|---|---|---|
| Order Form acknowledged by (Name in capital letters) | [redacted] | Telephone | [redacted] |
| Supplier Name | **PA CONSULTING SERVICES LTD** | Email | [redacted] |
| Supplier Role / Position | [redacted] | Date | **11 June 2024** |
| Approver's signature | [redacted] | | |

## 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: [redacted]

## 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 Fin FAAMET 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 Air Freight Centre
IMPORTS 030 679 81113 / 81114 Fax 0117 913 8943
EXPORTS 030 679 81113 / 81114 Fax 0117 913 8943
Surface Freight Centre
IMPORTS 030 679 81129 / 81133 / 81138 Fax 0117 913 8946
EXPORTS 030 679 81129 / 81133 / 81138 Fax 0117 913 8946 **B.**
**JSCS**

JSCS Helpdesk No. 01869 256052 (select option 2, then option 3)
JSCS Fax No. 01869 256837
Users requiring an account to use the MOD Freight Collection Service should contact [redacted] in the first instance.

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

**(b) U.I.N.**

| | |
|---|---|
| **5. Drawings/Specifications are available from** | **11. The Invoice Paying Authority**<br>Ministry of Defence 0151-242-2000 DBS Finance<br>Walker House, Exchange Flags Fax: 0151-242-2809<br>Liverpool, L2 3YL **Website is:**<br>https://www.gov.uk/government/organisations/ministryofdefence/about/procurem |
| **6. Intentionally Blank** | **12. Forms and Documentation are available through *:**<br>Ministry of Defence, Forms and Pubs Commodity Management<br>PO Box 2, Building C16, C Site |
| | Lower Arncott<br>Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)<br>**Applications via fax or email:**<br>[redacted] |
| **7. Quality Assurance Representative:**<br><br>Commercial staff are reminded that all Quality Assurance requirements should be listed under the General Contract Conditions.<br><br>**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]. | *** NOTE**<br>**1.** Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Intern Site: https://www.kid.mod.uk/maincontent/business/commer cial/index.htm<br><br>**2.** If the required forms or documentation are not available on the MOD Intern site requests should be submitted through the Commercial Officer named Section 1. |

**Appendix 1 to Schedule 6**

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

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

1. To: 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 |
|---|---|---|---|---|---|---|
| | | | | 0 | | |
| | | | | 0 | | |
| | | | | 0 | | |
| | | | | 0 | | |
| | | | | 0 | | |

*If the Authority choses to implement the optional extension a Contract Change notice will be put in place to outline the Manpower required for that extension.

| 5b. Travel | (Estimated expenditure on:) | Unit cost | Number of Journeys / Miles | Total |
|---|---|---|---|---|
| | Rail | 0 | | 0 |
| | Motor Mileage (max 30p per mile incl VAT) | 30p max (incl VAT) | 0 | 0 |
| | Air | 0 | | 0 |
| | Sea | 0 | | 0 |
| 5c. Subsistence | (Estimated expenditure on:) | Unit cost | Number of Night / Days | Total |
| | Accommodation (max £100 per night incl VAT) | 0 | 0 | 0 |
| | Meals (max £5 for lunch and/or £22.50 for an evening meal, including all drinks | 0 | 0 | 0 |
| | | 0 | 0 | 0 |

| | | |
|---|---|---|
| 5d.Other Costs | Miscellaneous costs (please define below) | The above T&S costs relate to the period to |
| | **Subcontractor price** | |
| | Subcontractor Details | |
| | Materials | |
| | Other<br>(Please provide details below)<br>Description | Cost |
| Total Charges | completion of Call-Off Contract Deliverables | …… (excl. VAT) |

**Appendix 3**

Not used.

**Appendix 4 (Template Statement of Work)**

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

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

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

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

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

**Date of SOW:**

**SOW Title:**

**SOW Reference:**

**Call-Off Contract Reference:**

**Requirement Holder:**

**Supplier:**

**SOW Start Date:**

**SOW End Date:**

**Duration of SOW:**

**Key Personnel (Requirement Holder):**

**Key Personnel (Supplier):**

**Subcontractors:**

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

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

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

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

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

**Outcome Description:**

| Milestone Ref | Milestone Description | Acceptance Criteria | Due Date |
|---|---|---|---|
| MS01 | | | |
| MS02 | | | |

**Delivery Plan:**

**Dependencies:**

**Supplier Resource Plan:**

**Security Applicable to SOW:**

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

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

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

**SOW Standards:**

[Insert any specific Standards applicable to this SOW]

**Performance Management:**

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

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

| Material KPIs | Target | Measured by |
|---|---|---|
| | | |
| | | |

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

**Additional Requirements:**

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

**Key Supplier Staff:**

| Key Role | Key Staff | Contract Details | Employment / Engagement Route **(incl. inside/outside IR35)** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**SOW Reporting Requirements:**

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

| Ref. | Type of Information | Which Deliverables does this requirement apply to? | Required regularity of Submission |
|---|---|---|---|
| 1. | [insert] | | |
| 1.1 | [insert] | [insert] | [insert] |

**4. Charges**

**Call Off Contract Charges:**

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

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

[Requirement Holder to select as appropriate for this SOW]

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

Rate Cards Applicable:

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

**Reimbursable Expenses:**

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

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

[None]

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

**5. Signatures and Approvals**

**Agreement of this SOW**

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

**For and on behalf of the Supplier**

Name:

Title:

Date:

Signature:

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

Name:

Title:

Date:

Signature:

**Annex 1 to Statement of Work**

**Data Processing**

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**<br>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:<br>**N/A**<br><br>**The Supplier is Controller and the Relevant Authority is Processor**<br>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: **N/A**<br><br>**The Parties are Joint Controllers**<br>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: **N/A**<br><br>**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:<br><br>● Business contact details of Supplier Personnel for which the Supplier is the Controller,<br>● 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, |
| Duration of the Processing | From the contract start date until the contract end date. |
| Nature and purposes of the Processing | 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). |
| Type of Personal Data | Names, Email Addresses, Telephone Numbers |
| Categories of Data Subject | Personnel (including volunteers, agents, and temporary workers), customers/ clients and suppliers |

**Appendix 5**

**Confidentiality Undertaking**

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

Employee:

Name of Employer:

MOD Contract/Task No:

Title:

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

may include particularly commercially sensitive information), whether documentary, electronic, aural or in any other form, belonging to or controlled by the Secretary of State for Defence or third parties. I may also become aware, as a result of my work in connection with the Contract, of other information concerning the business of the Secretary of State for Defence or third parties, which is by its nature confidential.

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

3. Unless otherwise instructed by my Employer, if I have in the course of my employment received documents, software or other materials from the Secretary of State for Defence or other third party for the purposes of my duties under the above Contract then I shall promptly return them to the Secretary of State for Defence or third party (as the case may be) at the completion of the Contract via a representative of my Employer who is an authorised point of contact under the Contract and (in the case of information referred to under paragraph 1 above) is also authorised under paragraph 2. Alternatively, at the option of the Secretary of State for Defence or the third party concerned, I shall arrange for their proper destruction and notify the above authorised point of contact under the Contract to supply a certificate of destruction to the Secretary of State for Defence. Where my Employer may legitimately retain materials to which this paragraph applies after the end of the Contract, I shall notify the authorised representative of my Employer to ensure that they are stored, and access is controlled in accordance with my Employer's rules concerning third party confidential information.

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

Signed:

Date:

**Appendix 6**

**Security Aspects Letter**

Secretary of State for Defence, acting by the Directorate of the UK Strategic Command, Defence Digital,
Building 405,
MOD Corsham, Westwells Road,
Corsham,
Wiltshire, SN13 9NR

**Date of Issue:** 19/04/2024

**For the attention of:**

[redacted]

PA Consulting Services Ltd

**ITT/CONTRACT NUMBER & TITLE: PS439 - Digital Policy Service**

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

| ASPECTS | CLASSIFICATION |
|---|---|
| Material released in support of the execution of this contract will include project and programme documentation that has sensitive aspects. This may include electronic, physical documentation and discussions at meetings. | Official Sensitive |

(Note: Add more rows as required)

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

[redacted]

Copy via email to:

[redacted]

**ANNEX C: UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS**

**Purpose**

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority [redacted]

**Definitions**

2. The term *"Authority"* for the purposes of this Annex means the HMG Contracting Authority.

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

**Security Grading**

4. The SENSITIVE caveat is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all UK OFFICIAL and UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grad ing.

**Security Conditions**

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

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

6. The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other

conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

7. Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to register the IT system onto the Defence Assurance Risk Tool (DART). Details on the registration process can be found in the 'Industry Security Notices (ISN)' on

Gov.UK website. ISNs 2017/01, 04 and 06, Defence Condition 658 and Defence Standard 05-138 details the DART registration, IT security accreditation processes, risk assessment/management and Cyber security requirements which can be found in the following links:

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

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

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

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

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

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

**Access**

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

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

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

**Hard Copy Distribution**

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

16. Advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE shall be sought from the Authority. **Electronic Communication and Telephony and Facsimile Services**

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

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

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

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

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

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

**Use of Information Systems**

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

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

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

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

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

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

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

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

c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be *"strong"* using an appropriate method to achieve this, e.g. including numeric and *"special"* characters (if permitted by the system) as well as alphabetic characters.
d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 16 above.

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

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

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

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

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

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

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

(1). Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations),

(2). Defined Business Contingency Plan,
(3). Data backup with local storage,
(4). Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software),
(5). Operating systems, applications and firmware should be supported,
(6). Patching of Operating Systems and Applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

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

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

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

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

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

**Laptops**

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

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites [1]. For the avoidance of doubt the term *"drives"* includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

27. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

28. Portable CIS devices holding the Authorities' data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

**Loss and Incident Reporting**

29. The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIALSENSITIVE material to the Authority. In addition any loss or otherwise compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) below. This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD WARP will also advise the Contractor what further action is required to be undertaken.

**JSyCC WARP Contact Details**

30. Reporting instructions for any security incidents involving MOD classified material can be found in Industry Security Notice 2017/03 as may be subsequently updated at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf

**Sub-Contracts**

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

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

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf

33. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 30 above to the sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

**Publicity Material**

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

**Physical Destruction**

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

**Interpretation/Guidance**

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

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

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

**Audit**

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

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

**Appendix 7**

**Statement of Requirements – see Appendix 3**