DBS Mil Pers & Vets, SPO and DCDS (MilCap) Commercial Delivery Team

Contract No:702910453

Emerging Capabilities and Whole Force Futures Study

Between the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland **Team Name and address:** **DBS Mil Pers & Vets, SPO and DCDS (MilCap) Commercial Delivery Team** **Innsworth House, Imjin Barracks, Gloucester GL3 1HW**	**And** **Contractor Name and address:** Cranfield University Medway 5 College Road Bedford MK43 0AL

Contract Terms and Conditions

Table of Contents

Contents

SC1A (Edn 02/22) - MOD Terms and Conditions For Less Complex Requirements

Standardised Contracting Terms

1 Definitions - In the Contract:

The Authority means the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland, (referred to in this document as "the Authority"), acting as part of the Crown;

Business Day means 09:00 to 17:00 Monday to Friday, excluding public and statutory holidays;

Contract means the agreement concluded between the Authority and the Contractor, including all terms and conditions, associated purchase order, specifications, plans, drawings, schedules and other documentation, expressly made part of the agreement in accordance with Clause 2.c;

Contractor means the person, firm or company specified as such in the purchase order. Where the Contractor is an individual or a partnership, the expression shall include the personal representatives of the individual or of the partners, as the case may be;

Contractor Deliverables means the goods and / or services including packaging (and supplied in accordance with any QA requirements if specified) which the Contractor is required to provide under the Contract in accordance with the schedule to the purchase order;

Effective Date of Contract means the date stated on the purchase order or, if there is no such date stated, the date upon which both Parties have signed the purchase order;

Firm Price means a price excluding Value Added Tax (VAT) which is not subject to variation;

Government Furnished Assets (GFA) is a generic term for any MOD asset such as equipment, information or resources issued or made available to the Contractor in connection with the Contract by or on behalf of the Authority;

Hazardous Contractor Deliverable means a Contractor Deliverable or a component of a Contractor Deliverable that is itself a hazardous material or substance or that may in the course of its use, maintenance, disposal, or in the event of an accident, release one or more hazardous materials or substances and each material or substance that may be so released;

Issued Property means any item of Government Furnished Assets (GFA), including any materiel issued or otherwise furnished to the Contractor in connection with the Contract by or on behalf of the Authority;

Legislation means in relation to the United Kingdom any Act of Parliament, any subordinate legislation within the meaning of section 21 of the Interpretation Act 1978, any exercise of

Royal Prerogative or any enforceable community right within the meaning of Section 2 of the European Communities Act 1972.

Notices means all notices, orders, or other forms of communication required to be given in writing under or in connection with the Contract;

Parties means the Contractor and the Authority, and Party shall be construed accordingly;

Sensitive Information means the information listed as such in the purchase order, being information notified by the Contractor to the Authority, which is acknowledged by the Authority as being sensitive, at the point at which the Contract is entered into or amended (as relevant) and remains sensitive information at the time of publication;

Transparency Information means the content of this Contract in its entirety, including from time to time agreed changes to the Contract, except for (i) any information which is exempt from disclosure in accordance with the provisions of the Freedom of Information Act 2000 (FOIA) or the Environmental Information Regulations Act 2004 (EIR), which shall be determined by the Authority, and (ii) any Sensitive Information.

2 General

a. The Contractor shall comply with all applicable Legislation, whether specifically referenced in this Contract or not.

b. Any variation to the Contract shall have no effect unless expressly agreed in writing and signed by both Parties.

c. If there is any inconsistency between these terms and conditions and the purchase order or the documents expressly referred to therein, the conflict shall be resolved according to the following descending order of priority:

(1) the terms and conditions;

(2) the purchase order; and

(3) the documents expressly referred to in the purchase order.

d. Neither Party shall be entitled to assign the Contract (or any part thereof) without the prior written consent of the other Party.

e. Failure or delay by either Party in enforcing or partially enforcing any provision of the Contract shall not be construed as a waiver of its rights or remedies. No waiver in respect of any right or remedy shall operate as a waiver in respect of any other right or remedy.

f. The Parties to the Contract do not intend that any term of the Contract shall be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 by any person that is not a Party to it.

g. The Contract and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with English Law, and subject to Clause 15 and without prejudice to the dispute resolution procedure set out therein, the Parties submit to the exclusive jurisdiction of the English courts. Other jurisdictions may apply solely for the purpose of giving effect to this Clause 2.g and for enforcement of any judgement, order or award given under English jurisdiction.

3 Application of Conditions

a. The purchase order, these terms and conditions and the specification govern the Contract to the entire exclusion of all other terms and conditions. No other terms or conditions are implied.

b. The Contract constitutes the entire agreement and understanding and supersedes any previous agreement between the Parties relating to the subject matter of the Contract.

4 Disclosure of Information

Disclosure of information under the Contract shall be managed in accordance with DEFCON 531 (SC1).

5 Transparency

a. Notwithstanding any other condition of this Contract, and in particular Clause 4, the Contractor understands that the Authority may publish the Transparency Information to the general public.

b. Subject to clause 5.c, the Authority shall publish and maintain an up-to-date version of the Transparency Information in a format readily accessible and reusable by the general public under an open licence where applicable.

c. If, in the Authority's reasonable opinion, publication of any element of the Transparency Information would be contrary to the public interest, the Authority shall be entitled to exclude such information from publication. The Authority acknowledges that it would expect the public interest by default to be best served by publication of the Transparency Information in its entirety. Accordingly, the Authority acknowledges that it shall only exclude Transparency Information from publication in exceptional circumstances and agrees that where it decides to exclude information from publication on that basis, it will provide a clear statement to the general public explaining the categories of information that have been excluded from publication and reasons for withholding that information.

d. The Contractor shall assist and co-operate with the Authority as reasonably required to enable the Authority to publish the Transparency Information, in accordance with the principles set out above. Where the Authority publishes Transparency Information, it shall:

(1) before publishing redact any information that would be exempt from disclosure if it was the subject of a request for information under the FOIA and/or the EIR , for the avoidance of doubt, including Sensitive Information;

(2) taking into account the Sensitive Information set out in the purchase order, consult with the Contractor where the Authority intends to publish information which has been identified as Sensitive Information. For the avoidance of doubt the Authority, acting reasonably, shall have absolute discretion to decide what information shall be published or be exempt from disclosure in accordance with the FOIA and/or EIR; and

(3) present information in a format that assists the general public in understanding the relevance and completeness of the information being published to ensure the public obtain a fair view on how this Contract is being performed.

6 Notices

a. A Notice served under the Contract shall be:

(1) in writing in the English Language;

(2) authenticated by signature or such other method as may be agreed between the Parties;

(3) sent for the attention of the other Party's representative, and to the address set out in the purchase order;

(4) marked with the number of the Contract; and

(5) delivered by hand, prepaid post (or airmail), facsimile transmission or, if agreed in the purchase order, by electronic mail.

b. Notices shall be deemed to have been received:

(1) if delivered by hand, on the day of delivery if it is the recipient's Business Day and otherwise on the first Business Day of the recipient immediately following the day of delivery;

(2) if sent by prepaid post, on the fourth Business Day (or the tenth Business Day in the case of airmail) after the day of posting;

(3) if sent by facsimile or electronic means:

(a) if transmitted between 09:00 and 17:00 hours on a Business Day (recipient's time) on completion of receipt by the sender of verification of the transmission from the receiving instrument; or

(b) if transmitted at any other time, at 09:00 on the first Business Day (recipient's time) following the completion of receipt by the sender of verification of transmission from the receiving instrument.

7 Intellectual Property

a. The Contractor shall as its sole liability keep the Authority fully indemnified against an infringement or alleged infringement of any intellectual property rights or a claim for Crown use of a UK patent or registered design caused by the use, manufacture or supply of the Contractor Deliverables.

b. The Authority shall promptly notify the Contractor of any infringement claim made against it relating to any Contractor Deliverable and, subject to any statutory obligation requiring the Authority to respond, shall permit the Contractor to have the right, at its sole discretion to assume, defend, settle or otherwise dispose of such claim. The Authority shall give the Contractor such assistance as it may reasonably require to dispose of the claim and will not make any statement which might be prejudicial to the settlement or defence of the claim

8 Supply of Contractor Deliverables and Quality Assurance

a. This Contract comes into effect on the Effective Date of Contract.

b. The Contractor shall supply the Contractor Deliverables to the Authority at the Firm Price stated in the Schedule to the purchase order.

c. The Contractor shall ensure that the Contractor Deliverables:

(1) correspond with the specification;

(2) are of satisfactory quality (within the meaning of the Sale of Goods Act 1979, as amended) except that fitness for purpose shall be limited to the goods being fit for the particular purpose held out expressly by or made known expressly to the Contractor and in this respect the Authority relies on the Contractor's skill and judgement; and

(3) comply with any applicable Quality Assurance Requirements specified in the purchase order.

d. The Contractor shall apply for and obtain any licences required to import any material required for the performance of the Contract in the UK. The Authority shall provide to the Contractor reasonable assistance with regard to any relevant defence or security matter arising in the application for any such licence.

9 Supply of Data for Hazardous Contractor Deliverables

a. The Contractor shall establish if the Contractor Deliverables are, or contain, Dangerous Goods as defined in the Regulations set out in this Clause 9. Any that do shall be packaged for UK or worldwide shipment by all modes of transport in accordance with the following unless otherwise specified in the Schedule to the purchase order:

(1) the Technical Instructions for the Safe Transport of Dangerous Goods by Air (ICAO), IATA Dangerous Goods Regulations;

(2) the International Maritime Dangerous Goods (IMDG) Code;

(3) the Regulations Concerning the International Carriage of Dangerous Goods by Rail (RID); and

(4) the European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR).

b. Certification markings, incorporating the UN logo, the package code and other prescribed information indicating that the package corresponds to the successfully designed type shall be marked on the packaging in accordance with the relevant regulation.

c. As soon as possible and in any event within the period specified in the purchase order (or if no such period is specified no later than one month prior to the delivery date), the Contractor shall provide to the Authority's representatives in the manner and format prescribed in the purchase order:

(1) confirmation as to whether or not to the best of its knowledge any of the Contractor Deliverables are Hazardous Contractor Deliverables; and

(2) for each Hazardous Contractor Deliverable, a Safety Data Sheet containing the data set out at Clause 9.d, which shall be updated by the Contractor during the period of the Contract if it becomes aware of any new relevant data.

d. Safety Data Sheets if required under Clause 9.c shall be provided in accordance with the extant UK REACH Regulation and any additional information required by the Health and Safety at Work etc. Act 1974 and shall contain:

(1) information required by the Classification, Labelling and Packaging (GB CLP) Regulation or any replacement thereof; and

(2) where the Hazardous Contractor Deliverable is, contains or embodies a radioactive substance as defined in the extant Ionising Radiation Regulations, details of the activity, substance and form (including any isotope); and

(3) where the Hazardous Contractor Deliverable has magnetic properties, details of the magnetic flux density at a defined distance, for the condition in which it is packed.

e. The Contractor shall retain its own copies of the Safety Data Sheets provided to the Authority in accordance with Clause 9.d for 4 years after the end of the Contract and shall make them available to the Authority's representatives on request.

f. Nothing in this Clause 9 reduces or limits any statutory or legal obligation of the Authority or the Contractor.

g. Where delivery is made to the Defence Fulfilment Centre (DFC) and / or other Team Leidos location / building, the Contractor must comply with the Logistic Commodities and Services Transformation (LCST) Supplier Manual.

10 Delivery / Collection

a. The purchase order shall specify whether the Contractor Deliverables are to be delivered to the consignee by the Contractor or collected from the consignor by the Authority.

b. Title and risk in the Contractor Deliverables shall pass from the Contractor to the Authority

on delivery or on collection in accordance with Clause 10.a.

c. The Authority shall be deemed to have accepted the Contractor Deliverables within a reasonable time after title and risk has passed to the Authority unless it has rejected the Contractor Deliverables within the same period.

11 Marking of Contractor Deliverables

a. Each Contractor Deliverable shall be marked in accordance with the requirements specified in the purchase order. or if no such requirement is specified, the Contractor shall mark each Contractor Deliverable clearly and indelibly in accordance with the requirements of the relevant DEF-STAN 05-132 as specified in the contract or specification. In the absence of such requirements, the Contractor Deliverables shall be marked with the MOD stock reference, NATO Stock Number (NSN) or alternative reference number shown in the Contract.

b. Any marking method used shall not have a detrimental effect on the strength, serviceability or corrosion resistance of the Contractor Deliverables.

c. The marking shall include any serial numbers allocated to the Contractor Deliverable.

d. Where because of its size or nature it is not possible to mark a Contractor Deliverable with the required particulars, the required information should be included on the package or carton in which the Contractor Deliverable is packed, in accordance with condition 12 (Packaging and Labelling (excluding Contractor Deliverables containing Ammunition or Explosives)).

12 Packaging and Labelling of Contractor Deliverables (Excluding Contractor Deliverables Containing Ammunition or Explosives)

The Contractor shall pack or have packed the Contractor Deliverables in accordance with any requirements specified in the purchase order and Def Stan 81-041 (Part 1 and Part 6).

13 Progress Monitoring, Meetings and Reports

The Contractor shall attend progress meetings and deliver reports at the frequency or times (if any) specified in the purchase order and shall ensure that its Contractor's representatives are suitably qualified to attend such meetings. Any additional meetings reasonably required shall be at no cost to the Authority.

14 Payment

a. Payment for Contractor Deliverables will be made by electronic transfer and prior to submitting any claims for payment under clause 14b the Contractor will be required to register their details (Supplier on-boarding) on the Contracting, Purchasing and Finance (CP&F) electronic procurement tool.

b. Where the Contractor submits an invoice to the Authority in accordance with clause 14a, the Authority will consider and verify that invoice in a timely fashion.

c. The Authority shall pay the Contractor any sums due under such an invoice no later than a period of 30 days from the date on which the Authority has determined that the invoice is valid and undisputed.

d. Where the Authority fails to comply with clause 14b and there is undue delay in considering and verifying the invoice, the invoice shall be regarded as valid and undisputed for the purpose of clause 14c after a reasonable time has passed.

e. The approval for payment of a valid and undisputed invoice by the Authority shall not be construed as acceptance by the Authority of the performance of the Contractor's obligations nor as a waiver of its rights and remedies under this Contract.

f. Without prejudice to any other right or remedy, the Authority reserves the right to set off any amount owing at any time from the Contractor to the Authority against any amount payable by the Authority to the Contractor under the Contract or under any other contract with the Authority, or with any other Government Department.

15 Dispute Resolution

a. The Parties will attempt in good faith to resolve any dispute or claim arising out of or relating to the Contract through negotiations between the respective representatives of the Parties having authority to settle the matter, which attempts may include the use of any alternative dispute resolution procedure on which the Parties may agree.

b. In the event that the dispute or claim is not resolved pursuant to Clause 15.a the dispute shall be referred to arbitration and shall be governed by the Arbitration Act 1996. For the purposes of the arbitration, the arbitrator shall have the power to make provisional awards pursuant to Section 39 of the Arbitration Act 1996.

c. For the avoidance of doubt it is agreed between the Parties that the arbitration process and anything said, done or produced in or in relation to the arbitration process (including any awards) shall be confidential as between the Parties, except as may be lawfully required in judicial proceedings relating to the arbitration or otherwise. No report relating to anything said, done or produced in or in relation to the arbitration process may be made beyond the tribunal, the Parties, their legal representatives and any person necessary to the conduct of the proceedings, without the concurrence of all the Parties to the arbitration.

16 Termination for Corrupt Gifts

The Authority may terminate the Contract with immediate effect, without compensation, by giving written notice to the Contractor at any time after any of the following events:

a. where the Authority becomes aware that the Contractor, its employees, agents or any sub-contractor (or anyone acting on its behalf or any of its or their employees):

(1) has offered, promised or given to any Crown servant any gift or financial or other advantage of any kind as an inducement or reward;

(2) commits or has committed any prohibited act or any offence under the Bribery Act 2010 with or without the knowledge or authority of the Contractor in relation to this Contract or any other contract with the Crown;

(3) has entered into this or any other contract with the Crown in connection with which commission has been paid or has been agreed to be paid by it or on its behalf, or to its knowledge, unless before the contract is made particulars of any such commission and of the terms and conditions of any such agreement for the payment thereof have been disclosed in writing to the Authority.

b. In exercising its rights or remedies to terminate the Contract under Clause 16.a. the Authority shall:

(1) act in a reasonable and proportionate manner having regard to such matters as the gravity of, and the identity of the person committing the prohibited act;

(2) give due consideration, where appropriate, to action other than termination of the Contract, including (without being limited to):

(a) requiring the Contractor to procure the termination of a subcontract where the prohibited act is that of a Subcontractor or anyone acting on its or their behalf;

(b) requiring the Contractor to procure the dismissal of an employee (whether its own or that of a Subcontractor or anyone acting on its behalf) where the prohibited act is that of such employee.

c. Where the Contract has been terminated under Clause 16.a.the Authority shall be entitled to purchase substitute Contractor Deliverables from elsewhere and recover from the Contractor any costs and expenses incurred by the Authority in obtaining the Contractor Deliverables in substitution from another supplier.

17 Material Breach

In addition to any other rights and remedies, the Authority shall have the right to terminate the Contract (in whole or in part) with immediate effect by giving written notice to the Contractor where the Contractor is in material breach of its obligations under the Contract. Where the Authority has terminated the Contract under Clause 17 the Authority shall have the right to claim such damages as may have been sustained as a result of the Contractor's material breach of the Contract.

18 Insolvency

The Authority shall have the right to terminate the contract if the Contractor is declared bankrupt or goes into liquidation or administration. This is without prejudice to any other rights or remedies under this Contract.

19 Limitation of Contractor's Liability

a. Subject to Clause 19.b the Contractor's liability to the Authority in connection with this Contract shall be limited to £5m (five million pounds).

b. Nothing in this Contract shall operate to limit or exclude the Contractor's liability:

(1) for:

a. any liquidated damages (to the extent expressly provided for under this Contract);

b. any amount(s) which the Authority is entitled to claim, retain or withhold in relation to the Contractor's failure to perform or under-perform its obligations under this Contract, including service credits or other deductions (to the extent expressly provided for under this Contract);

c. any interest payable in relation to the late payment of any sum due and payable by the Contractor to the Authority under this Contract;

d. any amount payable by the Contractor to the Authority in relation to TUPE or pensions to the extent expressly provided for under this Contract;

(2) under Condition 7 of the Contract (Intellectual Property), and DEFCONs 91 or 638 (SC1) where specified in the contract;

(3) for death or personal injury caused by the Contractor's negligence or the negligence of any of its personnel, agents, consultants or sub-contractors;

(4) for fraud, fraudulent misrepresentation, wilful misconduct or negligence;

(5) in relation to the termination of this Contract on the basis of abandonment by the Contractor;

(6) for breach of the terms implied by Section 2 of the Supply of Goods and Services Act 1982; or

(7) for any other liability which cannot be limited or excluded under general (including

statute and common) law.

c. The rights of the Authority under this Contract are in addition to, and not exclusive of, any rights or remedies provided by general (including statute and common) law.

20 The project specific DEFCONs and DEFCON SC variants that apply to this Contract are:

DEFCON 129J (SC1)
DEFCON 129J (SC1) (Edn 06/17) – The Use of Electronic Business Delivery Form

DEFCON 503 (SC1)
DEFCON 503 (SC1) (Edn. 07/21) - Formal Amendments To Contract

DEFCON 531 (SC1)
DEFCON 531 (SC1) (Edn. 09/21) - Disclosure of Information

DEFCON 532B
DEFCON 532B (Edn 04/20) - Protection of Personal Data

DEFCON 534
DEFCON 534 (Edn. 06/21) - Subcontracting and Prompt Payment

DEFCON 537
DEFCON 537 (Edn. 12/21) - Rights of Third Parties

DEFCON 538
DEFCON 538 (Edn. 06/02) - Severability

DEFCON 566
DEFCON 566 (Edn. 10/20) - Change of Control of Contractor

DEFCON 609
DEFCON 609 (SC1) (Edn.08/18) – Contractor's Records

DEFCON 620
DEFCON 620 (SC1) (Edn.08/21) – Contract Change Control Procedure

DEFCON 658 (SC1)
DEFCON 658 (SC1) (Edn. 09/21) – Cyber

Note: Further to DEFCON 658 (SC1) (Edn. 09/21) the Cyber Risk Profile of the Contract is **Moderate**, as defined in Def Stan 05-138.

DEFCON 659A
DEFCON 659A (Edn. 09/21) - Security Measures

DEFCON 660
DEFCON 660 (Edn. 12/15) - Official-Sensitive Security Requirements
DEFCON 703

DEFCON 703
(Edn 06/21) - Intellectual Property Rights - Vesting In The Authority

21 The special conditions that apply to this Contract are:

General Conditions

a. Third Party IPR Authorisation

AUTHORISATION BY THE CROWN FOR USE OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS

Notwithstanding any other provisions of the Contract and for the avoidance of doubt, award of the Contract by the Authority and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Contractor acknowledges that any such authorisation by the Authority under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.

b. Payment Terms

Payment will be made in accordance with clause 14 following completion and acceptance of the milestones detailed in the Schedule of Requirements.

c. Quality Assurance Conditions

No Specific QMS

No Specific Quality Management System requirements are defined. This does not relieve the Supplier of providing conforming Products under this Contract.

d. Government Furnished Information (GFI)

‘The Authority does not give any warranty or undertaking as to the completeness, accuracy, or fitness for any purpose of any of the Authority provided information. Neither the Authority nor its agents or employees shall be liable to the contractor in contract (save as expressly provided elsewhere in the Contract), tort, statute nor otherwise, as a result of any inaccuracy, omission, unfitness for any purpose, or inadequacy of any kind, in the Authority provided information.’

e. Security Aspects Letter and additional Security Conditions

This requirement is subject to the Security Aspects Letter (SAL) reference “702910453 SAL” dated 08 June 2022 and additional Security Conditions detailed at Annex C to the SAL.

22 The processes that apply to this Contract are:

A DEFFORM 316 (EDN05/98) Government Furnished Information will be completed for all GFI provided under this contract. Completed DEFFORM 316’s will form part of the contract.

Schedule 1 - Additional Definitions of Contract

Schedule 1 - Additional Definitions of Contract

There are no additional definitions of Contract.

Purchase Order

PURCHASE ORDER

SC1A PO
(Edn 02/22)

Contract No: 702910453

Contract Name: Emerging Capabilities and Whole Force Futures Study

Dated: 08 June 2022

Supply the Deliverables described in the Schedule to this Purchase Order, subject to the attached MOD Terms and Conditions for Less Complex Requirements (up to the applicable procurement threshold).

Contractor	**Quality Assurance Requirement (Clause 8)**
Name: Cranfield University Registered Address: College Road Cranfield Bedfordshire MK43 0AL	

Consignor (if different from Contractor's registered address)	**Transport Instructions (Clause 10)**
Name: Not Applicable Address:	Select method of transport of Deliverables To be Delivered electronically by the Contractor to: The Authority ~~To be Collected by the Authority~~ Each consignment of the Deliverables shall be accompanied by a delivery note.

Progress Meetings (Clause 13)	**Progress Reports (Clause 13)**
The Contractor shall be required to attend the following meetings: Subject: Progress Meetings Frequency: If required, as requested by the Project Manager detailed in the DEFFORM 111. Location: Virtually	The Contractor is required to submit the following Reports: Subject: Progress Report Frequency: If required, as requested by the Project Manager detailed in the DEFFORM 111 Method of Delivery: Electronically Delivery Address: To the Project Manager detailed in the DEFFORM 111
Payment (Clause 14)	

Payment is to be enabled by CP&F.

Forms and Documentation	**Supply of Hazardous Deliverables (Clause 9)**
Forms can be obtained from the following websites: https://www.aof.mod.uk/aofcontent/tactical/toolkit (Registration is required). https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#invoice-processing https://www.dstan.mod.uk/ (Registration is required). The MOD Forms and Documentation referred to in the Conditions are available free of charge from: Ministry of Defence, Forms and Pubs Commodity Management PO Box 2, Building C16, C Site Lower Arncott Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824) Applications via email: Leidos-FormsPublications@teamleidos.mod.uk If you require this document in a different format (i.e. in a larger font) please contact the Authority's Representative (Commercial Officer), detailed below.	A completed DEFFORM 68 and, if applicable, Safety Data Sheet(s) are to be provided by email with attachment(s) in Adobe PDF or MS WORD format to: a. The Commercial Officer detailed in the Purchase Order, and b. DESTECH-QSEPEnv-HSISMulti@mod.gov.uk by the following date: 6 July 2022 or if only hardcopy is available to the addresses below: Hazardous Stores Information System (HSIS) Defence Safety Authority (DSA) Movement Transport Safety Regulator (MTSR) Hazel Building Level 1, #H019 MOD Abbey Wood (North) Bristol BS34 8QW

Contractor Sensitive Information (Clause 5). Not to be published. This list shall be agreed in consultation with the Authority and the Contractor and may be reviewed and amended by agreement. The Authority shall review the list before publication of any information.
Description of Contractor's Sensitive Information:
Cross reference to location of Sensitive Information:
Explanation of Sensitivity:
Details of potential harm resulting from disclosure:
Period of Confidence (if Applicable):
Contact Details for Transparency / Freedom of Information matters: Name: Position: Address: Telephone Number: E-mail Address:

Offer and Acceptance	
A) The Purchase Order constitutes an offer by the Contractor to supply the Deliverables. This is open for acceptance by the Authority for days from the date of signature. By signing the Purchase Order the Contractor agrees to be bound by the attached Terms and Conditions for Less Complex Requirements (Up to the applicable procurement threshold). Name (Block Capitals): Position: For and on behalf of the Contractor Authorised Signatory …….. Date:	B) Acceptance Name (Block Capitals): Position: For and on behalf of the Authority Authorised Signatory …….. Date:
C) Effective Date of Contract: 28 June 2022	

Schedule Of Requirements

SCHEDULE OF REQUIREMENTS FOR THE EMERGING CAPABILITIES AND WHOLE FORCE FUTURES STUDY

Deliverables									
Item Number	**MOD Stock Reference No.**	**Part No. (where applicable)**	**Specification**	**Consignee Address Code** (full address is detailed in DEFFORM 96)	**Packaging Requirements inc. PPQ and DofQ** (as detailed in DEFFORM 96)	**Delivery Date**	**Total Qty**	**Firm Price (£) Ex VAT**	
								Per Item	**Total inc. packaging (and delivery if specified in the Purchase Order)**
1	N/A	N/A	Phase 1 – Horizon Scanning	N/A	N/A	30 October 2022	1		
2	N/A	N/A	Phase 2 – Adapting Existing Scenarios up to the production and acceptance of the Final Report	N/A	N/A	28 February 2023	1		
								Total Firm Price	£85,000

Item Number	**Consignee Address (XY code only)**
1-2	Delivery details to be agreed with the project team prior to delivery

Annex A to Schedule 2 - Statement Of Requirement for 702910453 – Emerging Capabilities And Whole Force Futures Study

Background.

A horizon scanning study on the impact of emerging military capabilities and future changes in the Whole Force is required as part of the FMC Infra Futures Programme. This study is needed to inform Strategy for Defence Infrastructure (SDI) development and direction, and strategic planning. Any evidence gathered may also inform future Strategic Defence and Security Review (SDSR)/Spending Review (SR) rounds. The output will also help support strategic direction and management of interdependencies between the regular, reserve, training and overseas estates, supporting the Public Account Committee (PAC) recommendation.

Our estate infrastructure is a critical enabler of Defence capability and outputs. Approximately 1.8% of the UK landmass is managed or used by MOD, comprising airfields, barracks, naval bases, nuclear facilities, warehouses, workshops, offices, training areas, test ranges, housing and community facilities. Expenditure accounts for approximately 12% of the Defence budget (as of 2019/2020).

The Defence estate and infrastructure may need to respond to significant change in the next 30 years relating to emerging capabilities and the future Whole Force, to effectively enable Defence capabilities and operations. The rapid evolution of emerging Defence capabilities, e.g., cyber, space, and robotics will have a demand on infrastructure which may need to be met by either the adaption of existing or the building new facilities or new bespoke infrastructure.

<u>Constraints:</u>

- Budgetary constraints – Budgetary constraints such as those of Top Level Budgets (TLBs) may constrain how infrastructure can adapt to emerging capabilities and changes in the Whole Force.
- Policy constraints – Although the future may be significantly different to today, the policy aims of today's Government (including MOD and relevant Other Government Departments' policies) provides direction and constraints on what type of future is desirable. The supplier shall consider current policy aims, so this project's reports and scenario development consider how actions can be taken over the next several years and next few decades to increase the likelihood of a desirable future that delivers the Government's policy aims.

Completion of the study is dependent on information being provided by relevant MOD stakeholders. FMC Infra shall provide the supplier with a stakeholder contacts list.

Requirement. The requirement is for a horizon scanning study on the impact of emerging military capabilities and future changes in the Whole Force to be undertaken.

Description of Work and Deliverables.

The work involves the following phases.

1. Horizon scanning:
    - Implications of emerging military capabilities (all domains - land, air, maritime, space, cyber and "support")

- Implications of changes in the future Whole Force (composition and structure) may have implications for the Defence estate and infrastructure e.g. geographical location, building standards, demand for accommodation, messing, size of the Whole Force, structure and composition, the expectations of future generations, etc.

The deliverable will be a horizon scanning report. This report shall be reviewed by FMC Infra prior to acceptance of this deliverable.

2. Development of Futures scenarios that cover two epochs: 2021-2030 (to reflect current capability and infra planning and IR/SR outcomes) and 2045-2050.

   The deliverable will be a scenarios workshop; a scenarios report on the key drivers & trends, implications for Defence sector and the Whole Force; and a synthesis report. The reports shall be reviewed by FMC Infra prior to acceptance of these deliverables.

The following criteria should be considered for horizon scanning, and where relevant, for the development of scenarios:

- **Infrastructure Requirements.** Will the capability require new bespoke infrastructure or can use adapted/upgraded existing assets?
- **Use of the Reserve and Training Estate and airspace.** Will there likely be a change in amount and type of use of the Reserve and Training Estate and airspace above MOD establishments?
- **Overseas basing.** Will there be a continued requirement to forward base capability overseas, and in which areas?
- **Supporting Requirements.** Will the capability require changes in fuel requirements, energy upgrades, comms, storage or warehousing etc.? Might there be increased requirements to use buildings on the Defence estate for 3D printing of replacement parts for platforms (or other new technological activities) whilst also reducing the need for warehouse space to store spare parts, as there might be global trends in the use of 3D printing to support military capabilities[1].
- **Capability responsibility or organisational transformation.** Could the capability require a change in responsibility or require organisational transformation that may have implications for the Defence estate e.g. creation of a Space Command.
- **Dependencies with other capabilities or domains.** Consider multi-domain integration, which also includes alignment across Government, integration with allies, integrating military and non-military capabilities, and considering dependencies on the private sector. How future platforms might be more likely to be interlinked meaning that the infrastructure that supports them may need to be managed as a system-of systems.[2]

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025139/RAND_RRA1309-1.pdf

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025139/RAND_RRA1309-1.pdf

- **Multi-role platforms –** In future, there might be greater use of multi-role platforms.[3] Also, the Defence and Security Industrial Strategy refers to multi-role aircraft and ships.[4]
- **Whole Force.** What will be the implications for the Whole Force? Future numbers; military/civilian/contactor mix; role of the civilian sector in delivering and operating capabilities offsite. This may influence demand for accommodation, welfare facilities etc.
- **Impact of locations on capabilities/geographic footprint.** Whether a change in the Defence footprint will be required (e.g. increased need for specific environments such as urban, littoral etc., the requirement to recruit and retain certain skill sets such as cyber, programming and the availability of those skills in different locations, devolution policies.)
- **Sustainability.** Any sustainability (including environmental and social) impacts relating to emerging capabilities and future Whole Force requirements for infrastructure.

Emerging Capabilities include but are not limited to: Cyber; Space; Communications; Electromagnetic, Robotics; Augmented Reality (AR)/Virtual Reality (VR); Machine learning/Automation; Simulation; Synthetic training; Unmanned Aerial Vehicles (UAVs)/swarm technologies; Disposable technologies; Power, fuel and battery technologies.

Key performance indicators:

- Production of high-quality reports that include a wide range of evidence, including information from MOD stakeholders, and considers the accuracy/credibility of the evidence, highlighting where there are uncertainties or contradictory evidence.
- Knowledge transfer – The supplier shall work with FMC Infra to transfer knowledge of horizon scanning and scenario development methodologies and approaches to FMC Infra.
- Continuous improvement – The supplier shall work with FMC Infra to continuously improve as the project progresses, such as by suggesting new approaches and methodologies to use, adapting an approach to improve engagement with MOD stakeholders, and identifying new areas that they could investigate in addition to the criteria in the above list.

Contract Start Date and Duration. The proposed start date is Feb 2021. The contract duration is nine months.

Security Considerations.

- Products/reports produced by the supplier shall contain the relevant protective marking. There is a requirement for there to be a means of electronically exchanging OFFICIAL-SENSITIVE information with the supplier.
- Any engagement that the supplier conducts with external (outside MOD) stakeholders to gather evidence shall be conducted in a way that does not disclose sensitive information without the authority to do so. FMC Infra is to be engaged with if the supplier is unsure of what information can be discussed with external stakeholders.
- The supplier (every contractor who will be working on the project) shall ensure that they understand the requirements of the Official Secrets Act, comply with it, and sign the Official Secrets Act and Confidentiality Declaration (MOD Form 134).

---

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025139/RAND_RRA1309-1.pdf

[4] https://www.gov.uk/government/publications/defence-and-security-industrial-strategy

Other Considerations.

- **Government Furnished Equipment/Information (GFE/GFI)**.
    - The GFI that will be provided are a contacts list of stakeholders for the supplier to engage with; and information from MOD stakeholders about military capabilities, areas relating to the Whole Force, and any other relevant areas.
    - A Security Aspects Letter (SAL) is required.

Project Deliverables and Milestones

Phases of Work	**Deliverable**	**Milestone Date**
Phase 1 - Horizon scanning. Structured horizon scanning to develop an understanding of changing demands on infrastructure due to emerging capabilities and the future Whole Force, so that this can be planned for more efficiently and earlier on. This will include an assessment of the implications of emerging military capabilities (all domains - land, air, maritime, space, cyber and "support"), and also the implications of changes in the composition and structure of the future Whole Force (e.g. geographical location, building standards, demand for accommodation, messing, size of the Whole Force, structure and composition, the expectations of future generations, etc.).	**Draft report:** Trends, implications, cross-cutting themes report.	**31/09/2022**
	Final report: Trends, implications, cross-cutting themes report. This report will follow internal QA and client review.	**30/10/2022**
Phase 2 - Adapting existing scenarios. Adapt a number of existing plausible future scenarios that explore core uncertainties in the defence and security landscape in the UK. Apply the scenarios to consider the implications for military capabilities and the composition and structure of the Whole Force, the Defence estate and infrastructure.	**Interim review / summary report:** Adapted scenarios; key drivers & trends.	**31/12/2022**
	Draft report: Adapted scenarios, key drivers & trends, implications for military capabilities and Whole Force (composition and structure)	**31/01/2023**
	Final report: Adapted scenarios, key drivers & trends, implications for military capabilities and Whole Force (composition and structure)	**28/02/2023**

Deliverables

Deliverables Note

This matrix is intended to provide an overview of the parties' contractual obligations to assist with contract management. It does not form part of the contract and should not be relied upon to aid interpretation of the contract. In the event of any conflict, inconsistency or discrepancy between this matrix and the contract, the terms of the contract shall take precedence.

Negotiation Deliverables

All Negotiation Deliverables

Supplier Contractual Deliverables

Name	Description	Due	Responsible Party
Payment Condition 14.c	Payment		Supplier Organization
Payment Condition 14.b	Submission of Invoices		Supplier Organization
Import Licences Condition 8.d	Apply for and obtain all necessary licences		Supplier Organization
Marking of Hazardous Deliverables Condition 9.b	Ensure packaging is marked in accordance with the contract		Supplier Organization

Buyer Contractual Deliverables

Name	Description	Due	Responsible Party
Termination Condition 16, 17, 18	Written notice of Termination due to corrupt Gifts as stipulated in the contract		Buyer Organization
Notification of Claim Condition 7.b	Notify contractor of any third party claim and assist the contractor to dispose of said claim		Buyer Organization
Import Licences Condition 8.d	Assist application for licences that are defence/security related		Buyer Organization

DEFFORM 111

Appendix - 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:

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

4. Supply / Support Management Branch or Order Manager:

(a) Branch/Name:

(b) U.I.N.

5. Drawings/Specifications are available from

6. Intentionally Blank

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

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

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
Tel. 44 (0) 161 233 5397

2. For all other enquiries contact DES Fin FA-AMET Policy, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
Tel. 44 (0) 161 233 5394

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

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

EXPORTS Tel. 030 679 81113 / 81114 Fax 0117 913 8943
Surface Freight Centre
IMPORTS Tel. 030 679 81129 / 81133 / 81138 Fax 0117 913 8946
EXPORTS Tel. 030 679 81129 / 81133 / 81138 Fax 0117 913 8946

B.JSCS

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

11. The Invoice Paying Authority

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

12. Forms and Documentation are available through *:

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

*** NOTE**

1. Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Internet Site: https://www.aof.mod.uk/aofcontent/tactical/toolkit/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.

DEFFORM 532

Personal Data Particulars

DEFFORM 532
Edn 10/19

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

Data Controller	The Data Controller is the Secretary of State for Defence (the Authority). The Personal Data will be provided by: Delivery team name: FMC Infrastructure Delivery team address: MOD Head Office | 1B MOD Main Building | Horse Guards Avenue | London | SW1A 2HB (Because of a planned floorplate move, it is expected that after early May 2022, the address will change to: MOD Head Office | 3D MOD Main Building | Horse Guards Avenue | London | SW1A 2HB)
Data Processor	The Data Processor is the Contractor. The Personal Data will be processed at: Cranfield University, College Road, Cranfield, MK43 0AL
Data Subjects	The Personal Data to be processed under the Contract concern the following Data Subjects or categories of Data Subjects: *[please specify]* MOD/Defence staff, including: •Defence strategies: SPO Strategy Hub, FMC Capability Strategy, Climate Change and Sustainability directorate, Defence Intelligence, DIO Estate Strategy, ACDS RF&C. •Infrastructure: FMC Infrastructure Capability, TLB Infrastructure branches, RFCA, DIO (Regional Delivery, Capability, Customer Support team, Accommodation, Training Estate). •Capabilities: FMC Capability Plans, FMC Joint Plans, FMC Infra, FMC Space directorate, FMC Strategic Programmes, Climate Change and Sustainability directorate, Defence Support, Defence Digital, Oil and Pipelines Agency. •People: DIO, Dstl, People Strategy, People Accommodation •Science and technology: DST, Dstl, DIO (D Ex, Technical Services, Capability). Any external stakeholders who also agree to provide input who have given consent for their name and email address to be shared with the Contractor

Categories of Data	The Personal Data to be processed under the Contract concern the following categories of data: Name Email address Contact details in email signatures (work address, phone number, etc) if provided by individuals in emails with the Contractor Opinions/perspectives provided through interview *[Examples include name, address, telephone number, medical records etc]*
Special Categories of data (if appropriate)	The Personal Data to be processed under the Contract concern the following Special Categories of data: Not applicable *[A Special Category of Personal Data is anything that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation or genetic or biometric data]*
Subject matter of the processing	The processing activities to be performed under the contract are as follows: *[please specify]* Phase 1: Information about changes in infrastructure capabilities, science & technology and worker/demographic change will be collated via the web and through key informant interviews and assessed to interpret implications for emerging military capabilities and the composition and structure of the Work force. Phase 2: Similar information above will be collated and interpreted in a stakeholder workshop to explore core uncertainties in the defence and security landscape in the UK. Outputs from the workshop will be synthesised by core project team to produce alternative future scenarios. The scenarios will be used to consider the implications for military capabilities and the composition and structure of the Whole Force, the Defence estate and infrastructure. The latter may require running either a workshop or conducting interviews with stakeholders to interpret scenarios. *[This should be a high-level, short description of what processing will be taking place and its overall outcome i.e. its subject matter]*
Nature and the purposes of the Processing	The Personal Data to be processed under the Contract will be processed as follows: The nature of the processing will be the 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 by automated means or not).

Technical and organisational measures	The following technical and organisational measures to safeguard the Personal Data are required for the performance of this Contract: Security-cleared staff, that have been pre-agreed with the sponsor, will have access to the initial data and data-gathering exercise. All of which have agreed to be bound by the additional Local information security procedures, in addition to the standard policies, procedures and processed in place for University staff. All access to data will be through individually assigned accounts, and data will be processed in an accredited environment using pre-defined University-managed devices. If additional access by other University staff is required this will only be permitted subject to pre-agreement with the sponsor and the acceptance of the applicable Local information security procedures.
Instructions for disposal of Personal Data	The disposal instructions for the Personal Data to be processed under the Contract are as follows (where Disposal Instructions are available at the commencement of Contract): Retention –Interview data for 1 year, the remainder to be specified in the contract (all transcripts will be password-protected) Disposal – As specified in the contract Specific email inbox will be created for the duration of the project and accessed by authorised personnel only *Before the contract end date, emails about the project that have been sent by the Contractor to stakeholders (including MOD, Oil and Pipelines Agency, UK Hydrographic Office, US Visiting Forces and any external stakeholders) will be forwarded to the FMC Infrastructure team when the contract is completed, so that Government information can be kept to fulfil legal requirements such as future Freedom of Information requests, and so that the information can be available to relevant MOD staff who 'need to know' the process behind how the project was carried out. After the emails have been forward to FMC Infrastructure team, the Contractor shall delete their emails with the personal data before the contract end date (this includes deleting emails from the Deleted Items folder and deleting the emails from any locations where it is possible to recover the emails that have been deleted from the Deleted Items such as the 'Recover items recently removed from this folder' location).*
Date from which Personal Data is to be processed	Where the date from which the Personal Data will be processed is different from the Contract commencement date this should be specified here: To be determined (probably early June 2022)

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

FMC Infrastructure Assistant Head Strategy
FMC Infra
MOD Abbey Wood (North)
Oak, Level 2 East Wing, Mailpoint #6201
Bristol
BS34 8QW

Our reference: 702910453 SAL

Date: 08 June 2022

For the personal attention of:

Christopher Buckland
Cranfield University
Medway 5
College Road
Bedford
MK43 0AL
securitycontroller@cranfield.ac.uk

Dear Sir,

SECURITY ASPECTS LETTER
FOR: 702910453 - Emerging Capabilities and Whole Force Futures Study

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 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition, see Annex C, outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

Item no.	Item description	Classification to be considered
1.	Existence of project.	OFFICIAL
2.	Business card level details (e.g. names, roles, business email, etc).	OFFICIAL
3.	Project plans, progress reports, agendas, minutes of meetings, general client correspondence.	Up to OFFICIAL-SENSITIVE
4.	Information on current and future military capabilities, Whole Force, and infrastructure.	Up to OFFICIAL-SENSITIVE

5.	Draft versions of any Ministry of Defence or Other Government Department strategies, policies and/or guidance.	Up to OFFICIAL-SENSITIVE
6.	Information on any other topics that are related, indirectly related and/or not related to current and future military capabilities, Whole Force and infrastructure. (For example, information might be provided to explore whether activities in one policy area might affect current and future military capabilities, Whole Force or infrastructure, and it becomes apparent that the information is not related to the main topics of the study, and the information is not used in reports produced.)	Up to OFFICIAL-SENSITIVE

3. Information about this contract must not, without the approval of the Authority, be published or communicated to anyone except where necessary for the execution of the contract.

4. Your attention is drawn to the requirements of the 'Security Conditions' at Annexes B through H, and 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

5. The enclosed Security Conditions at Annex C outline the principal measures required to safeguard OFFICIAL-SENSITIVE information are provided to enable you to apply the required degree of protection.

6. If any security incidents occur to classified information regarding this contract, then it shall be reported in accordance the requirements laid down in Annex C.

7. The 'Need to Know' security principle is to be enforced rigorously at all times with regards to all project material (e.g., documentation, drawings, conversation).

8. 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 understood and that the requirements of this Security Aspects Letter and the UK Security Conditions will be complied with using the Acceptance letter at Annex A.

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.

9. 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.

10. Classified Information associated with this Contract must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

11. The Contractor shall ensure that all individuals (contractors, sub-contractors and agency personnel) working on Defence Contracts must apply the requirements of HMG Baseline Personnel Security Standard (Minimum BPSS)[1]. The contracting company should be able to demonstrate that the checks have been carried out satisfactorily and are in place and that such checks may be audited, and spot checked by the contracting organisation.

Yours faithfully,

Annexes:

A. Acceptance of Security Aspects Letter (SAL) - To be returned to the Authority with the signed SC1 Purchase Order.
B. Technical Grading Guide for Official Sensitive material
C. OFFICIAL-SENSITIVE Security Condition for UK Contracts.
D. Official Secrets Act section 2.
E. SAL Acknowledgment Sheet for Employees or Subcontracts

Copy to:

ISAC-Group (MULTIUSER)
SPO DSR-IIPCSy (MULTIUSER)
ISS Des-DAIS-SRAAcc4-IA

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/677553/HMG_Baseline_Personnel_Security_Standard.pdf

Annex A to 702901453 SAL
Dated: 08 June 2022

ACCEPTANCE OF SECURITY ASPECTS LETTER (SAL)

1. Receipt of the above SAL is acknowledged. On behalf of the contractor, I confirm that:

   a. The content within Annexes B to D, together with all the security requirements described within this SAL, is understood. This content is to be briefed to all personnel who will be working on this contract / task and all sub-contractors, who require access to project information.

   b. The classified information, within Annexes B to D, has been brought to the attention of the person directly responsible for the security of this contract. This will include supplying suitable SALs and references to your sub-contractors.

   c. Copies of all sub-contractor SALs will be sent to the undersigned or their representative.

   d. Measures will be taken to safeguard the Controlled Material and/or OFFICIAL-SENSITIVE / OFFICIAL Matter in line with procedures approved by the Head Office Principal Security Advisor team.

   e. Individuals 'need to know' and access requirements in relation to the project information are strictly role-based, and therefore, automatically rescinded on job change or departure.

   f. All conditions and requirements above in this SAL will be complied with.

Signed[5] …… Date ……

Name …… Job Title ……..

[5] To be signed by the Project Director only. Remaining project staff are to sign Annex I.

Annex B to 702901543 SAL
Dated: 08 June 2022

TECHNICAL GRADING GUIDE FOR OFFICIAL SENSITIVE INFORMATION

Item no.	Item description	Classification to be considered	Remarks
1.	Existence of project	OFFICIAL	Shared on a need to know basis in line with Official Secrets Act
2.	Business card level details (e.g. names, roles, business email, etc)	OFFICIAL	Shared on a need to know basis in line with Official Secrets Act
3.	Project plans, progress reports, agendas, minutes of meetings, general client correspondence.	Up to OFFICIAL-SENSITIVE	Shared on a need to know basis in line with Official Secrets Act. Use of Defence Share, an accredited solution, or Win Zip for all OFFICIAL-SENSITIVE transmission of documents.
4.	Information on current and future military capabilities, Whole Force, and infrastructure.	Up to OFFICIAL-SENSITIVE	Shared on a need to know basis in line with Official Secrets Act. Use of Defence Share, an accredited solution, or Win Zip for all OFFICIAL-SENSITIVE transmission of documents.
5.	Draft versions of any Ministry of Defence or Other Government Department strategies, policies and/or guidance.	Up to OFFICIAL-SENSITIVE	Shared on a need to know basis in line with Official Secrets Act. Use of Defence Share, an accredited solution, or Win Zip for all OFFICIAL-SENSITIVE transmission of documents.
6.	Information on any other topics that are related, indirectly related and/or not related to current and future military capabilities, Whole Force and infrastructure. (For example, information might be provided to explore whether activities in one policy area might affect current and future military capabilities, Whole Force or infrastructure, and it becomes apparent that the information is not related to the main topics of the study, and the information is not used in reports produced.)	Up to OFFICIAL SENSITIVE	Shared on a need to know basis in line with Official Secrets Act. Use of Defence Share, an accredited solution, or Win Zip for all OFFICIAL-SENSITIVE transmission of documents.

Annex C to 702910453 SAL
Dated: 08 June 2022

ANNEX C: UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS[6]

Purpose

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: SPODSR-IIPCSy@mod.gov.uk).

Definitions

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

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

Security Grading

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

Security Conditions

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

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material

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

[6] JSP 440 Leaftet 13 Annex C (27/01/2022)

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/defence-condition-658-cyber-flow-down

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

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 17 above.

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites[7]. 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 OFFICIAL-SENSITIVE material to the Authority. In addition any loss or otherwise compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) below. This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD WARP will also advise the Contractor what further action is required to be undertaken.

JSyCC WARP Contact Details
Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)
RLI Email: defencewarp@modnet.rli.uk (MULTIUSER)
Telephone (Office hours): +44 (0) 30 6770 2185
JSyCC Out of hours Duty Officer: +44 (0) 7768 558863
Mail: JSyCC Defence Industry WARP
X007 Bazalgette Pavilion,
RAF Wyton, HUNTINGDON, Cambridgeshire, PE28 2EA.

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

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

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 31 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.

Annex D to 702910453 SAL
Dated: 08 June 2022

OFFICIAL SECRETS ACT SECTION 2

Defence

1. A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defence which is or has been in his possession by virtue of his position as such.

2. For the purposes of subsection 1. above, a disclosure is damaging if:

a. It damages the capability of, or of any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment or installations of those forces; or

b. Otherwise than as mentioned in paragraph a. above, it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or

c. It is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

3. It is a defense for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to Defence or that its disclosure would be damaging within the meaning of subsection 1. above.

4. In this section ‘Defence’ means:

a. The size, shape, organization, logistics, order of battle, deployment, operations, state of readiness and training of the armed forces of the Crown;

b. The weapons, stores or other equipment of those forces and the invention, development, production and operation of such equipment and research relating to it;

c. Defence policy and strategy and military planning and intelligence;

d. Plans and measures for the maintenance of essential supplies and services that are or would be needed in time of war.

Annex E to 702910453 SAL
Dated: 08 June 2022

SAL ACKNOWLEDGMENT SHEET

I confirm that I have read, understood, and will comply with:

I understand that the work on projects for contract **702910453** is of a sensitive nature and will only discuss specifics of the work with those that need to know for the delivery of the project.

I understand that failure to adhere to the Information Security management arrangements detailed in the above document or other documents referenced by it may result in disciplinary action being taken by the parent company; the revoking of my Security Clearance and site access and also potentially could lead to prosecution under the Official Secrets Act.

I understand that any questions regarding security should be directed to the Project Manager in the first instance.

Signed ……

Name …….

Date ……