Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	704626450
THE BUYER:	The Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland
BUYER ADDRESS	Navy Command Headquarters, Leach Building, Whale Island, Portsmouth, PO2 8BY
THE SUPPLIER:	Dentons UK and Middle East LLP
SUPPLIER ADDRESS:	One Fleet Place, London, EC4M 7WS
REGISTRATION NUMBER:	OC322045
DUNS NUMBER:	779522056
SID4GOV ID:	N/A

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 23 August 2022.

It's issued under the Framework Contract with the reference number RM6179 for the Provision of Short Term Legal Advice for BNSPS.

CALL-OFF LOT(S):

Lot 1 – General Legal Advice and Services

CALL-OFF INCORPORATED TERMS

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

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6179
3. The following Schedules in equal order of precedence:

   - **Joint Schedules for RM6179**
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)
     - Joint Schedule 4 (Commercially Sensitive Information)
     - Joint Schedule 10 (Rectification Plan)

   - **Call-Off Schedules for 704626450**
     - Call-Off Schedule 3 (Continuous Improvement)
     - Call-Off Schedule 7 (Key Supplier Staff)
     - Call-Off Schedule 17 (MOD Terms)
     - Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3.0.11)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6179

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.

CALL-OFF SPECIAL TERMS
The following Special Terms are incorporated into this Call-Off Contract:

IR35
IR35 off payroll working rules are not expected to apply to this requirement unless the Winning Tenderer indicates that the personnel who will be used to deliver Services will not be employed through their payroll. In those circumstances, a relevant assessment will be considered.

Cyber Risk
A Cyber Risk Assessment has been raised and the profile is Very Low. The reference is. A Supplier Assurance Questionnaire does need to be completed.

Where a Supplier Assurance Questionnaire needs to be completed, the Supplier must complete and email this to, Redacted under FOIA Section 40, Personal Information who will confirm cyber risk compliance. A copy of the completed questionnaire and the compliance email should then be returned to the Buyer.

If the Supplier's Supplier Assurance Questionnaire score does not meet the level set in the Cyber Risk Assessment, this may not prevent formation of a Call-Off Contract. In those circumstances, a Cyber Implementation Plan should be completed to demonstrate what actions will be taken to meet the required Cyber Risk level.

Provided the actions and timescales are considered acceptable to the Buyer, the Cyber Implementation Plan would then be included as a requirement in any resulting Call-Off Contract.

Cyber Implementation Plan Template

MOD contract number:	
CSM Risk Acceptance Reference:	
CSM Cyber Risk Profile:	
Name of Supplier:	
Current level of Supplier compliance:	
Reasons unable to achieve full compliance:	
Measures planned to achieve compliance / mitigate the risk with dates:	
Anticipated date of compliance / mitigations in place:	

Independent Controllers of Personal Data

1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

3. Where a Party has provided Personal Data to the other Party, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

5. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

(c) where it has recorded it in Annex 1 DEFFORM 532B (Personal Data Particulars) and Annex 1.1 (Processing Personal Data).

6. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

7. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

8. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party

that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

9. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

(e) Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 DEFFORM 532B (Personal Data Particulars) and Annex 1.1 (Processing Personal Data).

10. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 DEFFORM 532B (Personal Data Particulars) and Annex 1.1 (Processing Personal Data).

11. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

CALL-OFF START DATE: 30 August 2022

CALL-OFF EXPIRY DATE: 29 May 2023

CALL-OFF INITIAL PERIOD: 9 months

CALL-OFF OPTIONAL EXTENSION PERIOD: 9 months

CALL-OFF DELIVERABLES

The Buyer is entitled to 2 hours of free initial consultation and legal advice with each Order in accordance with Paragraph 5.2 of Framework Schedule 1 (Specification).

See details in Call-Off Schedule 20 (Call-Off Specification)

SECURITY
They Supplier will be required to comply with the requirements of the Security Aspects Letter at Annex A.

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms, and as amended by the Framework Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £60,000 + 50% = £90,000 (ex VAT and allowable expenses) and this shall be the Supplier's total limit of liability for this call-off order form dated 4 August 2022.

CALL-OFF CHARGES
The maximum hourly rate as set out in RM6179 Legal Services Panel Rate Card:

Partner	Redacted under FOIA Section 43, Commercial interests
Senior Associate	Redacted under FOIA Section 43, Commercial interests
Associate	Redacted under FOIA Section 43, Commercial interests

Hours billed will be invoiced on a monthly basis and itemised by activity and adviser. This will be cross checked with the Policy lead Redacted under FOIA Section 40, Personal Information

The contract value will be the limit of liability for the Buyer.

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law

REIMBURSABLE EXPENSES
Included within day rate charged.

DISBURSEMENTS
Not Payable

ADDITIONAL TRAINING CHARGE
Not applicable

SECONDMENT CHARGE
Not applicable

PAYMENT METHOD
Payment will be made electronically via the Exostar system and invoices will need to be submitted via this system to enable payment.

BUYER'S INVOICING ADDRESS:
Redacted under FOIA Section 40, Personal Information

BUYER'S AUTHORISED REPRESENTATIVE
Redacted under FOIA Section 40, Personal Information

BUYER'S ENVIRONMENTAL POLICY
Not Applicable

BUYER'S SECURITY POLICY
As per Security Aspects Letter and DEFCON658

BUYER'S ICT POLICY
See DEFCON658

SUPPLIER'S AUTHORISED REPRESENTATIVE
Redacted under FOIA Section 40, Personal Information

SUPPLIER'S CONTRACT MANAGER
Redacted under FOIA Section 40, Personal Information

PROGRESS REPORT
Not applicable.

PROGRESS MEETINGS AND PROGRESS MEETING FREQUENCY
To be arranged if and when required unless already detailed in Statement of Requirements.

KEY STAFF
Redacted under FOIA Section 40, Personal Information

KEY SUBCONTRACTOR(S)
Not Applicable

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off order Form and the Framework Terms.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	Redacted under FOIA Section 40, Personal Information	Signature:	Redacted under FOIA Section 40, Personal Information
Name:	Redacted under FOIA Section 40, Personal Information	Name:	Redacted under FOIA Section 40, Personal Information
Role:	Partner	Role:	Commercial Manager
Date:	25 August 2022	Date:	31st August 2022

Call-Off Schedule 17 (MOD Terms)

1 Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"MOD Terms and Conditions"	the terms and conditions listed in this Schedule;
"MOD Site"	shall include any of Her Majesty's Ships or Vessels and Service Stations;
"Officer in charge"	shall include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Officers superintending Government Establishments;

2 Access to MOD sites

2.1 The Buyer shall issue passes for those representatives of the Supplier who are approved for admission to the MOD Site and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Buyer and shall be surrendered on demand or on completion of the supply of the Deliverables.

2.2 The Supplier's representatives when employed within the boundaries of a MOD Site, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force for the time being for the conduct of staff at that MOD Site. When on board ship, compliance shall be with the Ship's Regulations as interpreted by the Officer in charge. Details of such rules, regulations and requirements shall be provided, on request, by the Officer in charge.

2.3 The Supplier shall be responsible for the living accommodation and maintenance of its representatives while they are employed at a MOD Site. Sleeping accommodation and messing facilities, if required, may be provided by the Buyer wherever possible, at the discretion of the Officer in charge, at a cost fixed in accordance with current Ministry of Defence regulations. At MOD Sites overseas, accommodation and messing facilities, if required, shall be provided wherever possible. The status to be accorded to the Supplier's staff for messing purposes shall be at the discretion of the Officer in charge who shall, wherever possible give his decision before the commencement of this Contract where so asked by the Supplier. When sleeping accommodation and messing facilities are not available, a certificate to this effect may be required by the Buyer and shall be obtained by the Supplier from the Officer in charge. Such certificate shall be presented to the Buyer with other evidence relating to the costs of this Contract.

2.4 Where the Supplier's representatives are required by this Contract to join or visit a Site overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided for them free of charge by the Ministry of Defence whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Supplier shall make such arrangements through the Technical Branch named for this purpose in the Buyer Contract Details. When such transport is not available within a reasonable time, or in circumstances where the Supplier wishes its representatives to accompany material for installation which it is to arrange to be delivered, the Supplier shall make its own transport arrangements. The Buyer shall reimburse the Supplier's reasonable costs for such transport of its representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Supplier's representatives locally overseas which is necessary for the purpose of this Contract shall be provided wherever possible by the Ministry of Defence, or by the Officer in charge and, where so provided, shall be free of charge.

2.5 Out-patient medical treatment given to the Supplier's representatives by a Service Medical Officer or other Government Medical Officer at a Site overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Site and transportation of the Supplier's representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Supplier at rates fixed in accordance with current Ministry of Defence regulations.

2.6 Accidents to the Supplier's representatives which ordinarily require to be reported in accordance with Health and Safety at Work etc. Act 1974, shall be reported to the Officer in charge so that the Inspector of Factories may be informed.

2.7 No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Supplier's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current Ministry of Defence rates.

2.8 The Supplier shall, wherever possible, arrange for funds to be provided to its representatives overseas through normal banking channels (e.g. by travellers' cheques). If banking or other suitable facilities are not available, the Buyer shall, upon request by the Supplier and subject to any limitation required by the Supplier, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made at the Site to which the Supplier's representatives are attached. All such advances made by the Buyer shall be recovered from the Supplier

3 DEFCONS and DEFFORMS

3.1 The DEFCONS and DEFORMS listed in Annex 1 to this Schedule are incorporated into this Contract.

3.2 Where a DEFCON or DEFORM is updated or replaced the reference shall be taken as referring to the updated or replacement DEFCON or DEFORM from time to time.

3.3 In the event of a conflict between any DEFCONs and DEFFORMS listed in the Order Form and the other terms in a Call Off Contract, the DEFCONs and DEFFORMS shall prevail.

4 Authorisation by the Crown for use of third party intellectual property rights

4.1 Notwithstanding any other provisions of the Call Off Contract and for the avoidance of doubt, award of the Call Off Contract by the Buyer 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 Supplier acknowledges that any such authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.

ANNEX 1 - DEFCONS & DEFFORMS

The full text of Defence Conditions (DEFCONs) and Defence Forms (DEFFORMS) are available electronically via https://www.gov.uk/guidance/knowledge-in-defence-kid.

The following MOD DEFCONs and DEFFORMs form part of this contract:

DEFCONs

DEFCON No	Version	Description
DEFCON 532B	(Edn 09/21)	Protection of Personal Data
DEFCON 658	SC1 (Edn 09/21) - Cyber	Further to DEFCON 658 the Cyber Risk Level of the Contract is Very Low, as defined in Def Stan 05-138

DEFFORMs (Ministry of Defence Forms)

DEFFORM No	Version	Description
DEFFORM 532	Edn 10/19	Personal Data Particulars

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: *Babcock Naval Service Pension Scheme (BNSPS) Trustees and their legal advisers Pinsent's*
Data Processor	The Personal Data will be processed at: *DENTONS, Dentons UK and Middle East LLP* *One Fleet Place, London, EC4M 7WS* *MOD's legal representatives in terms of the closure of the BNSPS.* Dentons acts as independent Data Controller
Data Subjects	The Personal Data to be processed under the Contract concern the following Data Subjects or categories of Data Subjects: Pension scheme beneficiaries *Information pertaining to members of the scheme who have a specific complaint or have been flagged as an anomaly in the wind up, information may include; Lengths of service, periods of non-pension accrual, previous employment, contracts worked under, age, gender.* *There will be **no need** to know names or identifying details.*
Categories of Data	The Personal Data to be processed under the Contract concern the following categories of data: *Identification information, contact details, Lengths of service, periods of non-pension accrual, previous employment, contracts worked under, age gender.*
Special Categories of data (if appropriate)	The Personal Data to be processed under the Contract concern the following Special Categories of data: *Not applicable*

Subject matter of the processing	The processing activities to be performed under the contract are as follows: *Information pertaining to members of the scheme who have a specific complaint or have been flagged as an anomaly in the wind up, information may include; Lengths of service, periods of non-pension accrual, previous employment, contracts worked under, age, gender.* *There will be **no need** to know names or identifying details, however personal data may inadvertently be part of documents shared across parties to be winding up of the scheme.* *Outcome is to resolve complaints and ensure smooth closure of the scheme.*
Nature and the purposes of the Processing	The Personal Data to be processed under the Contract will be processed as follows: *Personnel data, of provided will be for the express reason to provide advice on the best outcome for that individual in the case of the pension scheme wind up.*
Technical and organisational measures	The following technical and organisational measures to safeguard the Personal Data are required for the performance of this Contract: *Note minimal information will be sent to MOD and DENTONS which will be anonymised. DENTONS will not have access to non-anonymised data.*
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): *Data used to formulate advice will be archived on MOD systems in lieu of future questions and queries. DENTONs will be expected to delete any personnel, identifying data from their systems on completion of the contract.*
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: *30th August 2022*

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

ANNEX 1.1 - (Processing Personal Data)

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

The contact details of the Relevant Authority's Data Protection Officers are: Redacted under FOIA Section 40, Personal Information

1.1

The contact details of the Supplier's Data Protection Officer are: Redacted under FOIA Section 40, Personal Information

1.2

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**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: Provision of Short Term Legal Advice for Babcock Naval Service Pension Scheme (BNSPS)*
Duration of the Processing	*This will be for the duration of the Contract.*
Nature and purposes of the Processing	*Personnel data, of provided will be for the express reason to provide advice on the best outcome for that individual in the case of the pension scheme wind up.*
Type of Personal Data	*Information pertaining to members of the scheme who have a specific complaint or have been flagged as an anomaly in the wind up, information may include; Lengths of service, periods of non-pension accrual, previous employment, contracts worked under, age, gender.*

Categories of Data Subject	*Identification information, contact details, Lengths of service, periods of non-pension accrual, previous employment, contracts worked under, age gender.*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*Data used to formulate advice will be archived on MOD systems in lieu of future questions and queries.* *DENTONs will be expected to delete any personnel, identifying data from their systems on completion of the contract.*

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

Statement of Requirements

Dated: 31 May 2022

Statement Of Work Provided by Def Res

Continuation of Dentons Legal team in support of the Closure of the BNSPS pension scheme.

Background

Dentons has represented the MOD's equities in the HMT directed closure of the Babcock Naval Pensions Scheme (BNSPS). Redacted under FOIA Section 43, Commercial interests

Dentons had been paid through a previous Naval contract with Babcock, with the advice to the BNSPS scheme as part of that contract requirement. However, that contract has now ended, and new contract does not include any provision for this legacy scheme. Therefore, a mechanism is required to maintain Denton's Support whilst the scheme closes – projected March 23.

To provide for possible delays in closure, an option period of 9 months will be required.

Requirement

Work with the legal team of the other 2 parties in this issue (Babcock and the Trustees) to ensure that the Authority (MOD) is receiving information in regard to the scheme closure promptly and clearly.

Provide advice on documents received from Babcock and Trustees, in regard to the scheme and related issues.

Provide advice on issues that arise in regards the final stages of the closure of the of the scheme. Redacted under FOIA Section 43, Commercial interests

Advisers may be required to support senior engagements (PermSec, DG Finance or Ministers) or work alongside other SMEs (GAD) to develop coherent advice for the authority.

Advice will be limited to the BNSPS scheme Redacted under FOIA Section 43, Commercial interests

.

Support may be requested in terms of collecting wet signatures, photocopying and sending registry documents to ensure prover audit and timeline.

Advice should be provided verbally but where an audit trail to decision making is required written will be necessary.

Hours billed will be invoiced on a monthly basis and itemised by activity and adviser. This will be cross checked with the Policy lead Redacted under FOIA Section 40, Personal Information

Payment will be made electronically via the Exostar system and invoices will need to be submitted via this system to enable payment.

This requirement is expected to complete by April 23, with closure occurring in March and an additional month to complete any final paperwork.

An option period of a further 9 months, is required.

Summary

Given the complexity of this pension scheme closure, the proximity to the end point and the potential for future liabilities to MOD without legal support. It is recommended that the existing Legal advisers (Denton's) are maintained to provide legal advice to MOD. It is worth noting that Babcock (Clifford Chase) and the Trustees (Pinsents) are also in receipt of Legal representation.

ecurity Aspects Letter Redacted under FOIA Section 40, Personal Information

Ministry of Defence

Dentons UK and Middle East LLP
One Fleet Place
London
EC4M 7WS

Our Ref: 704626450

Date: 25 July 2022

For the personal attention of: Company Security Controller

Dear Sir / Madam

Contract Number & Title: 704626450: Short Term Legal Advice for BNSPS
Cyber Risk Assessment Reference: RAR-9V38OY67O

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

ASPECTS	CLASSIFICATION
Redacted under FOIA Section 43, Commercial interests	UK OFFICIAL-SENSITIVE

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 under FOIA Section 40, Personal Information

Copy via email to:

Redacted under FOIA Section 40, Personal Information

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 (Email: Redacted under FOIA Section 40, Personal Information

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

5. 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.

6. 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

7. 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.

8. 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.

9. 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.

10. 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.

11. 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

12. 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.

13. 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

14. 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.

15. 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

16. 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

17. 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.

18. 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.

19. 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

20. 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.

21. 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.

22. 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.

23. 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

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

25. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites . 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.

26. 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.

27. 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

28. 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
Redacted under FOIA Section 40, Personal Information
JSyCC Out of hours Duty Officer:
Mail: Redacted under FOIA Section 40, Personal Information

29. 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

30. 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.

31. 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 Security Policy Framework 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

32. 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

33. Contractors wishing to release any publicity material or display hardware 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

34. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when 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

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

36. 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

37. 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.