DPS Schedule 6 (Letter of Appointment and Order Schedules)

Letter of Appointment

This Letter of Appointment is issued in accordance with the provisions of the DPS Contract (708385450) between CCS and the Agency, dated February 2024.

Capitalised terms and expressions used in this letter have the same meanings as in the Order Incorporated Terms unless the context otherwise requires.

ORDER:

Order Number:	708385450
From:	Defence, Equipment & Support
To:	[Redacted]

Order Start Date:	01/04/2024
Order Expiry Date:	31/03/2026
Order Initial Period:	24 months
Order Optional Extension Period:	2 x 1 Year Options

Goods or Services required:	Services required in accordance within DPS Schedule 20 (Order Specification) of the DPS Agreement Subsequent calls for Tasking shall be priced and agreed using Schedule 25 (Tasking Form)

Key Staff:	**For the Buyer:** Project – [Redacted] Commercial – [Redacted] For the Supplier: [Redacted] [Redacted]

	[Redacted]
Guarantor(s)	N/A

Order Contract Charges (including any applicable discount(s), but excluding VAT):	Please refer to DPS Schedule 5 (Pricing Details)
Liability	The limitation of liability for this Order Contract is stated in Clause 11.1 of the Core Terms.
Additional Insurance Requirements	Not Applicable
Client billing address for invoicing:	[Redacted]

Special Terms	

PROGRESS REPORT FREQUENCY
Monthly service performance reports.

PROGRESS MEETING FREQUENCY
Monthly service reviews

KEY SUBCONTRACTOR(S)
N/A [Redacted] will not use key sub-contractors

COMMERCIALLY SENSITIVE INFORMATION
As Per Joint Schedule 4

SOCIAL VALUE COMMITMENT
The Contractor agrees, in providing the Requirements and performing its obligations under the Order Contract, that it will comply with the social value commitments.

SERVICE CREDIT CAP
This will be 100% of Monthly Support Fee in accordance with Schedule 5 (Order Pricing)

PAYMENT METHOD
The payment method for this Call-Off Contract is the Buyer's e-payment system "CP&F" (Contracting, Purchasing & Finance) system

BUYER'S INVOICE ADDRESS:
Invoices shall be submitted electronically via the Buyer's e-payment system "CP&F" (via Exostar)

ORDER INCORPORATED TERMS
The following documents are incorporated into this Order Contract. Where numbers are missing those schedules are not used. If the documents conflict, the following order of precedence applies:

1. This Letter of Appointment including the Order Special Terms and Order Special Schedules.
2. *Joint Schedule 1 (Definitions and Interpretation) RM6124*
3. *The following Schedules in equal order of precedence:*
    - *Joint Schedules for RM6124*
        - *Joint Schedule 4 (Commercially Sensitive Information)*
        - *Joint Schedule 6 (Key Subcontractors)*
        - *Joint Schedule 11 (Processing Data)*
    - *Order Schedules for 708385450*
        - *Order Schedule 1 (Transparency Reports)*
        - *Order Schedule 4 (Order Tender)*
        - *Order Schedule 5 (Pricing Details)*
        - *Order Schedule 14 (Service Levels)*
        - *Order Schedule 17 (MOD Terms)*
        - *Order Schedule 18 (Background Checks)*
        - *Order Schedule 20 (Order Specification)*

- *Order Schedule 24 (Security Aspects Letter)*
- *Order Schedule 25 (Tasking Form)*

4. CCS Core Terms

No other Agency terms are part of the Order Contract. That includes any terms written on the back of, or added to this Order Form, or presented at the time of delivery. For the avoidance of doubt, the relationship between the Parties is non-exclusive. The Client is entitled to appoint any other agency to perform services and produce goods which are the same or similar to the Goods or Services.

FORMATION OF ORDER CONTRACT

BY SIGNING AND RETURNING THIS LETTER OF APPOINTMENT (which may be done by electronic means) the Agency agrees to enter into an Order Contract with the Client to provide the Goods or Services in accordance with the terms of this letter and the Order Incorporated Terms.

The Parties hereby acknowledge and agree that they have read this letter and the Order Incorporated Terms. The Parties hereby acknowledge and agree that this Order Contract shall be formed when the Client acknowledges (which may be done by electronic means) the receipt of the signed copy of this letter from the Agency within two (2) Working Days from such receipt.

For and on behalf of the Agency:		**For and on behalf of the Client:**	
Signature:	[Redacted]	Signature:	[Redacted]
Name:	[Redacted]	Name:	[Redacted]
Role:	[Redacted]	Role:	[Redacted]
Date:	27th March 2024	Date:	20/3/2024

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

1.1 In this Schedule the Parties have sought to identify the Agency's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

Contractor's Sensitive Information

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 the publication of any information.

ITT Ref No: 708385450
Description of Contractor's Sensitive Information: [Redacted] provides certain information to you in connection with this procurement exercise which is confidential in nature and which is supplied to you strictly on the basis that it will be held in confidence. We have detailed the information below that we believe is exempt from the FOIA and therefore should not be published in the event of a request made under the FOIA or the proactive publishing of the won contract (including our tender response) in the event the contract is awarded to [redacted]: Personal information relating to our employees; we believe that this is exempt under S40 (2) of the FOIA to the extent that it constitutes personal data Information relating to our clients; in our opinion this is exempt under S41 FOIA as disclosure may constitute an actionable breach of confidence by our clients Information relating to our methodologies and systems; in our opinion this is exempt under S41 FOIA in that it is the basis for our unique offering. A detailed breakdown of our fees and other charges and our bank account details; we believe this is exempt under S43 FOIA as disclosure would prejudice our commercial interests
Cross Reference(s) to location of Sensitive Information in Tender: Tender response and commercial submission
Explanation of Sensitivity: As above
Details of potential harm resulting from disclosure: As above
Period of Confidence (if applicable): Duration of contract
Contact Details for Transparency / Freedom of Information matters: Name: [Redacted] Position: [Redacted]

Address: [Redacted] Telephone Number: [Redacted] Email Address: [Redacted]

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Agency is entitled to sub-contract its obligations under the DPS Contract to the Key Subcontractors identified on the Platform but this does not remove or reduce the Agency's liability for its performance of the Contract.

1.2 The Agency is entitled to sub-contract its obligations under an Order Contract to Key Subcontractors listed on the Platform who are specifically nominated in the Order Form but this does not remove or reduce the Agency's liability for its performance of the Contract.

1.3 Where during the Contract Period the Agency wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Client and the Agency shall, at the time of requesting such consent, provide CCS and the Client with the information detailed in Paragraph 1.4. The decision of CCS and the Client to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to the Platform. Where the Client consents to the appointment of a new Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. CCS and the Client may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Goods or Services or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

1.4 The Agency shall provide CCS and the Client with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

1.4.2 the scope/description of any Goods or Services to be provided by the proposed Key Subcontractor;

1.4.3 where the proposed Key Subcontractor is an Affiliate of the Agency, evidence that demonstrates to the reasonable satisfaction of the CCS and the Client that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;

1.4.4 for the Client, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Order Contract Period; and

1.4.5 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

1.5 If requested by CCS and/or the Client, within ten (10) Working Days of receipt of the information provided by the Agency pursuant to Paragraph 1.4, the Agency shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by CCS and/or the Client.

1.6 The Agency shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Agency to discharge its obligations under the Contracts including without limitation Order Schedule 15 (Order Contract Management);

1.6.2 a right under CRTPA for CCS and the Client to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Client respectively;

1.6.3 a provision enabling CCS and the Client to enforce the Key Sub-Contract as if it were the Agency;

1.6.4 a provision enabling the Agency to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Client;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Agency under the DPS Contract in respect of:

(a) the data protection requirements set out in Clause 14 (Data protection);

(b) the confidentiality requirements set out in Clause 15 (What you must keep confidential);

(c) the FOIA and other access request requirements set out in Clause 16 (When you can share information);

(d) the obligation not to embarrass CCS or the Client or otherwise bring CCS or the Client into disrepute;

(e) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

(f) the conduct of audits set out in Clause 6 (Record keeping and reporting);

1.6.6 provisions enabling the Agency to terminate the Key Sub-Contract on notice on terms no more onerous on the Agency than those imposed on CCS and the Client under Clauses 10.4 (When CCS or the Client can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Goods or Services provided to the Agency under the Key Sub-Contract without first seeking the written consent of CCS and the Client.

Joint Schedule 11 (Processing Data)

Definitions

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

"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Goods or Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*) unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Agency the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that:

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK

GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

7. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Personal Data Breach.

8. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Agency amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. 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.

19. 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.

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 of this Joint Schedule 11 above, 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.

21. 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.

22. 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 *(Processing Personal Data).*

23. 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.

24. 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.

25. 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.

26. 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.

27. 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 *(Processing Personal Data).*

28. 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 *(Processing Personal Data)*.

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Agency 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 27 of this Joint Schedule 11.

Annex 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.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: [Redacted]

1.2 The contact details of the Agency's Data Protection Officer are: [Redacted]

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 Relevant Authority is Controller and the Agency is Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Agency is the Processor of the following Personal Data: • Images of people used in the photography on the website, some of which is associated with employee profiles and some of which is staff images used in stock photography • Details stored in the website for the publishers (this is a small user group)
Duration of the Processing	For the term of this contract.
Nature and purposes of the Processing	For the purposes of providing the Services as per Schedule 20 (Order Specification)
Type of Personal Data	Email addresses
Categories of Data Subject	Staff, agents, suppliers

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 logs held in MOD Cloud by MoD

Order Schedule 1 (Transparency Reports)

1.1 The Agency recognises that the Client is subject to PPN 01/17 (Updates to transparency principles v1.1 (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Agency shall comply with the provisions of this Schedule in order to assist the Client with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Agency's reporting requirements set out in the DPS Contract, within three (3) Months of the Start Date the Agency shall submit to the Client for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Client rejects any proposed Transparency Report submitted by the Agency, the Agency shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Client. If the Parties fail to agree on a draft Transparency Report the Client shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Agency shall provide accurate and up-to-date versions of each Transparency Report to the Client at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Performance – in accordance with Schedule 14 (Service Levels)	Performance against Service Levels	To be provided in MS Word format with acceptance from the Project Manager	Monthly
Call-Off Contract Charges	Contract spend against contract value	Report	Monthly

Order Schedule 4 (Order Tender)

Social Value - Tackling economic inequality

[Redacted] – and our parent company, the [Redacted] – is proactively engaged in community and social initiatives. We are committed to supporting the wider agenda, which so many of our clients have at the core of their mission.

Below is a snapshot of our work; we'd be pleased to talk to you in more depth about how we can support your particular accessibility and social impact ambitions in the delivery of this contract. It can be a strategic workstream.

[Redacted] is a signatory of the **Care Leavers Covenant**. We participate in their national inclusion programme and have pledged support to individuals through provision of apprenticeships, work experience and other services with the ultimate aim of supporting care leavers to independence.

In 2021, [Redacted] launched the Group's **Levelling Up Action Plan** as a purpose-led organisation determined to have a positive social impact within the communities in which we and our clients work. This includes membership of the **Purpose Coalition** (https://www.purpose-coalition.org/). We are committed to help drive equality of opportunity for people and places with less opportunity, to break the cycle of Britain's endemic poor social mobility.

At a corporate level, we drive social impact through three interrelated pillars, with detailed, accountable workstreams.

[Redacted] is committed to excellence in corporate governance in line with the Wates Principles; our social impact initiatives form part of our annual reporting:

- Our ***Access to Work*** pillar uses our strengths to support people, whose working potential is currently under-realised.
- Under our ***Access to Opportunity*** pillar, we empower under-served youth by bringing our work closer to schools.
- Our ***Inclusive Futures*** pillar parallels our efforts internally to be an influencer in the recruitment industry, to drive diversity and inclusion for everyone.

Dedicated champion committees are in place across the business to drive these commitments with clear action plans. Just two examples:

Tackling Homelessness. We work with [Redacted] to transform the lives of people who have faced or are at risk of homelessness. We are a key funder and transformational partner of [Redacted] GROW programme, enabling people who have faced homelessness to use their experience and work for [Redacted]. We also support the partnership our extensive corporate network and colleagues' skills to get [Redacted] service users on their journey to sustainable employment.

Creating Brighter Futures Programme. This youth empowerment programme is designed to improve pre-employability and employability readiness for young people. With some of our key partners e.g. Enabling Enterprise, Skills Builder Partnership, CEC & CIPD – we focus on the relationship between young people's skills development, and life outcomes in terms of educational attainment, employment prospects, and social and emotional wellbeing.

Social Value - Fighting climate change

[Redacted] is part of the [Redacted] and benefits from the strength of Group-wide initiatives and contributes to ambitious goals and compliance measures in relation to CSR and environmental values. These are set out in the Group's S.172(1) statement in line with the Wates Principles.

Elevating environmental sustainability is a key strand of our first principle, Purpose and Leadership. This means that every leader in the business has the promotion of environmental values included within their role and performance standards.

Our environmental, social and governance (ESG) strategy is key to creating social and economic value for our clients, candidates, colleagues and the wider community – and ensures we safeguard our planet for future generations.

We regularly commission carbon footprint reports for the Group globally. Data on energy and greenhouse gas emissions in accordance with Streamlined Energy & Carbon Reporting (SECR) is included in the Directors' Report.

In early 2021, we anticipated that emerging from lockdown would increase our carbon footprint. We worked with an environmental impact consultant to agree specific focus areas for carbon reduction across the Group. These targets form the basis of a committee action plan to be delivered through three key project areas:

- Reducing travel, particularly by air. Sometimes travel is inevitable and necessary for business, but the pandemic proved the effectiveness of remote working and online;
- Moving all offices to electric heating systems and phasing out other forms of heating power, such as oil or gas, and switching all branch and office sites to electricity providers with a renewable 'green' electricity plan;
- Replacing Group company cars with electric models, starting with hybrid vehicles and ultimately looking to move to an all-electric fleet. [Redacted] itself does not have a company car policy; we offer a cycle to work scheme and subsidised travelcards.

Each focus group has a dedicated board sponsor; for [Redacted] this is our [Redacted]

The Environment Committee also set its short, medium and long-term goals for our business, incuding:

- To reduce our actual carbon output by 50% by 2030 (measured against our baseline level in 2019):
- To reduce our carbon output by 90% by 2050 (versus the same 2019 baseline) and eventually reach net-zero, using voucher offsetting as a last resort.

As an office-based service organisation, [Redacted] impact on the environment is low; since the pandemic, remote working has enabled us to deliver our services in evermore sustainable ways. We had always facilitated remote and e-enabled work, now the norm.

Nonetheless, we recognise the need to minimise this wherever possible and have adopted a policy to develop, implement and maintain an environmental management system that meets the requirements of ISO14001 and is re-visited regularly. In addition, our Purchasing Policy ensures we fully consider environmental issues throughout any procurement process.

We encourage clients to be similarly aware and will always propose ways of working that support environmental values – theirs and ours.

Social Value - Equal opportunity

[Redacted] has comprehensive policies in place relating to statutory responsibilities under the Equality Act 2010 (full copy available on request). Responsibility sits at SMT level with our [Redacted].

We are committed to equality at work – from our own recruitment through to development, reward and exiting. We oppose all forms of unlawful or unfair discrimination – direct/indirect and associative discrimination, harassment, harassment by a third party, victimisation and discrimination by perception including those on the grounds of any/all protected characteristics.

We treat all employees with dignity and respect and aim to provide a working environment free from all forms of discrimination. [Redacted] believes it is within our best interests, and those of all employees, to ensure the talents and skills available throughout the community are considered when employment opportunities arise.

We practice what we preach with regular training and insight sessions for every [Redacted] employee and an annual audit of our 200+ workforce. A snapshot from 2023:

- Gender: F64%; M35%; Nonbinary 0.5%
- Ethnicity: 26%
- Disability/Neurodiverse: 3%/0.5
- LGBTQ+: 9%

Beyond our legal responsibilities, however, [Redacted] is proactive in our aim to be at the forefront of diversity and inclusion best practice – not just in our own industry but overall. This benefits our business and drives our ability to offer our clients consultative, constructive challenge in their EDI activities and insights.

We are part of the [Redacted], one of the world's leading HR and recruitment services businesses. [Redacted] is represented on [Redacted] Diversity and Inclusion Committee. This has recently been strengthened with subject matter experts in corporate governance, communication, and learning and development. It encompasses stakeholders representing clients, candidates, colleagues and community.

Each focus group – Gender, Race and Ethnicity, LGBTQ+ and Accessibility – progresses specific initiatives. Examples include:

- Launch of LGBTQ+ UK and Ireland Network, where colleagues and allies discuss experiences and learn from each other. The forum hosts events such as Pride Month, Bisexual Visibility Day and Trans Awareness Week. We are reviewing internal policies to ensure they are LGBTQ+ inclusive and have launched our Allyship Programme.
- Our Gender Forum introduced the Group's menopause policy, which coincided with World Menopause Day and placed us within the forward-thinking 10% of companies with corporate guidance. We created a Manager's Toolkit and workshop series for colleagues and leaders.
- Our Accessibility Forum focus on mental health, signposting the Group's comprehensive support provision and encouraging involvement in Time to Talk Day.
- Our Race and Ethnicity Forum hosted a design-thinking workshop to give insight into what it's like to be a person of a Black, Asian or Multiple Ethnic background. Our Race

and Ethnicity Forum plan to create a mentoring programme, and review our internal data capture and monitoring

- [Redacted] equality work is designed, reported and measured in line with best practice in corporate governance.

Order Schedule 5 (Pricing Details)

Discovery Phase Milestone Payment

Year 1 Milestone	Delivery Date	Firm Price £(ex VAT)
Discovery Phase in accordance with Order Schedule 20 (Order Specification)	N/A	[Redacted]

The Discovery Phase is an opportunity for the Contractor to undertake due diligence to understand the codebase and Hosting Environment. If the Contractor after due diligence is unable to support the DE&S Website in accordance with Schedule 20 (Order Specification) the Authority will terminate the contract in accordance with the Core Terms. The Authority will pay actual costs incurred by the Contractor.

Support Services Payment Plan

Year 1 **Provision of a DE&S Internet Service Support service in accordance with Order Schedule 20 excluding additional services**	**DE&S Internet Support Service Fee Firm Price £(ex VAT)**
Month 1 Support Fee	[Redacted]
Month 2 Support Fee	[Redacted]
Month 3 Support Fee	[Redacted]
Month 4 Support Fee	[Redacted]
Month 5 Support Fee	[Redacted]
Month 6 Support Fee	[Redacted]
Month 7 Support Fee	[Redacted]
Month 8 Support Fee	[Redacted]
Month 9 Support Fee	[Redacted]
Month 10 Support Fee	[Redacted]
Month 11 Support Fee	[Redacted]
Month 12 Support Fee	[Redacted]
Total Ex VAT	**[Redacted]**

Year 2 **Provision of a DE&S Internet Service Support service in accordance with Order Schedule 20 excluding additional services**	**DE&S Internet Support Service Fee Firm Price £ (ex VAT)**
Month 1 Support Fee	[Redacted]
Month 2 Support Fee	[Redacted]
Month 3 Support Fee	[Redacted]
Month 4 Support Fee	[Redacted]
Month 5 Support Fee	[Redacted]
Month 6 Support Fee	[Redacted]
Month 7 Support Fee	[Redacted]
Month 8 Support Fee	[Redacted]
Month 9 Support Fee	[Redacted]

Month 10 Support Fee	[Redacted]
Month 11 Support Fee	[Redacted]
Month 12 Support Fee	[Redacted]
Total (Ex VAT)	**[Redacted]**

Support Services Payment Plan - Option Year 3

Option Year 3 **Provision of a DE&S Internet Service Support service in accordance with Order Schedule 20 excluding additional services**	**DE&S Internet Support Service Fee Firm Price £(ex VAT)**
Month 1 Support Fee	[Redacted]
Month 2 Support Fee	[Redacted]
Month 3 Support Fee	[Redacted]
Month 4 Support Fee	[Redacted]
Month 5 Support Fee	[Redacted]
Month 6 Support Fee	[Redacted]
Month 7 Support Fee	[Redacted]
Month 8 Support Fee	[Redacted]
Month 9 Support Fee	[Redacted]
Month 10 Support Fee	[Redacted]
Month 11 Support Fee	[Redacted]
Month 12 Support Fee	[Redacted]
Total Ex VAT	**[Redacted]**

Option Year 4 **Provision of a DE&S Internet Service Support service in accordance with Order Schedule 20 excluding additional services**	**DE&S Internet Support Service Fee Firm Price £ (ex VAT)**
Month 1 Support Fee	[Redacted]
Month 2 Support Fee	[Redacted]
Month 3 Support Fee	[Redacted]
Month 4 Support Fee	[Redacted]
Month 5 Support Fee	[Redacted]
Month 6 Support Fee	[Redacted]
Month 7 Support Fee	[Redacted]
Month 8 Support Fee	[Redacted]
Month 9 Support Fee	[Redacted]
Month 10 Support Fee	[Redacted]
Month 11 Support Fee	[Redacted]
Month 12 Support Fee	[Redacted]
Total (Ex VAT)	**[Redacted]**

Contractor Day Rate Card for pricing Tasking in accordance with Schedule 25 (Tasking Form)

Contract Years 1-2
Please provide your Day Rate Card for Contract Years 1 & 2

Level (cost per day) / Scope	Project Manager (ex VAT)	Back End Developer (ex VAT)	Data Migration Services (ex VAT)	Data Archiving Services (ex VAT)	Technical Subject Matter Expertise (ex VAT)	MoD Data Processing Activities (ex VAT)
SFIA 1 Follow	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 2 Assist	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 3 Apply	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 4 Enable	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 5 Ensure/Advise	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 6 Initiate/Influence	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 7 Set Strategy/Inspire	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Travel and Subsistence (T&S) – The day rates should not include T&S. T&S expenses will be based on a maximum day rate against a Limit of Liability. All T&S costs shall be on a reimbursement basis upon the Supplier providing valid receipts up to the limits specified in the Buyer's policy document "Ministry of Defence – Statement of Civilian Personnel Policy – Business Travel Guide V6.0-2022".

Option Years 3-4

Please provide your Day Rate Card for Contract for Option Year 3-4

Level (cost per day) / Scope	Project Manager (ex VAT)	Back End Developer (ex VAT)	Data Migration Services (ex VAT)	Data Archiving Services (ex VAT)	Technical Subject Matter Expertise (ex VAT)	MoD Data Processing Activities (ex VAT)
SFIA 1 Follow	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 2 Assist	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 3 Apply	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 4 Enable	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 5 Ensure/Advise	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 6 Initiate/Influence	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
SFIA 7 Set Strategy/Inspire	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Travel and Subsistence (T&S) – The day rates should not include T&S. T&S expenses will be based on a maximum day rate against a Limit of Liability. All T&S costs shall be on a reimbursement basis upon the Supplier providing valid receipts up to the limits specified in the Buyer's policy document "Ministry of Defence – Statement of Civilian Personnel Policy – Business Travel Guide V6.0-2022".

Order Schedule 14 (Service Levels)

1. Definitions

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

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Credits"	any service credits specified in the Annex to Part A of this Schedule being payable by the Agency to the Client in respect of any failure by the Agency to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Order Form;
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2. What happens if you don't meet the Service Levels

2.1 The Agency shall at all times provide the Goods or Services to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Agency acknowledges that any Service Level Failure shall entitle the Client to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Client as a result of the Agency's failure to meet any Service Level Performance Measure.

2.3 The Agency shall send Performance Monitoring Reports to the Client detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 A Service Credit shall be the Client's exclusive financial remedy for a Service Level Failure except where:

2.4.1 the Agency has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Agency;

(c) results in the corruption or loss of any Government Data; and/or

(d) results in the Client being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Client is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Client Termination Rights).

2.5 Not more than once in each Contract Year, the Client may, on giving the Agency at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Agency shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

2.5.2 the principal purpose of the change is to reflect changes in the Client's business requirements and/or priorities or to reflect changing industry standards; and

3. Critical Service Level Failure

3.1 On the occurrence of a Critical Service Level Failure

3.1.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.1.2 the Client shall be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Agency in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Client to terminate this Contract and/or to claim damages from the Agency for material Default.

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Agency:

- is likely to or fails to meet any Service Level Performance Measure; or
- is likely to cause or causes a Critical Service Failure to occur,

the Agency shall immediately notify the Client in writing and the Client, in its absolute discretion and without limiting any other of its rights, may:

1.a.1 require the Agency to immediately take all remedial action that is reasonable to mitigate the impact on the Client and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.a.2 instruct the Agency to comply with the Rectification Plan Process;

1.a.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Agency to the Client; and/or

1.a.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits

2.1 The Client shall use the Performance Monitoring Reports supplied by the Agency to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Goods or Services and do not include VAT. The Agency shall set-off the value of any Service Credits against the appropriate invoice in accordance with the calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

Service Levels			
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold
Accurate usage/ service reports & relevant billing schedule	Accuracy/ Timings	99%	Monthly service report agreed with the Client.
Available to provide technical support to resolve service incidents, problems, and requests 09:0017:00 Mon – Fri basis (excluding public holidays)	Availability of Penna Team	99%	[Redacted]available as indicated during core working hours.
Technical issues raised through Penna's designated online support site to be acknowledged within one hour	Timely acknowledgement	At least 98% at all times	Compliance via monthly reporting of issues to be shared at Monthly Service Review Meetings.
When Penna detects an incident before it has been reported by the Authority, it	Timely detection and notification	99%	Compliance with reporting and accepted by the DE&S Project Manager. Defined by active monitoring of incident) with notifications delivered via email to the

shall inform the Authority about incidents within 1 hour of occurrence			nominated DE&S point(s) of contact or mailbox(es).

The Service Credits shall be calculated on the basis of the following formula: Example:

Formula: x% (Service Level Performance Measure) - x% (actual Service Level performance)	=	x% of the Charges payable to the Client as Service Credits to be deducted from the next Invoice payable by the Client
Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period)	=	23% of the Charges payable to the Client as Service Credits to be deducted from the next Invoice payable by the Client]

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

3.1 Within twenty (20) Working Days of the Start Date the Agency shall provide the Client with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Agency shall provide the Client with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

3.2.3 details of any Critical Service Level Failures;

3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

3.2.6 such other details as the Client may reasonably require from time to time.

3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Agency and the Client of the Performance Monitoring Reports. The Performance Review Meetings shall:

3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Agency at such location and time (within normal business hours) as the Client shall reasonably require;

3.3.2 be attended by the Agency's Representative and the Client's Representative; and

3.3.3 be fully minuted by the Agency and the minutes will be circulated by the Agency to all attendees at the relevant meeting and also to the Client's Representative and any other recipients agreed at the relevant meeting.

3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Agency's Representative and the Client's Representative at each meeting.

3.5 The Agency shall provide to the Client such documentation as the Client may reasonably require in order to verify the level of the performance by the Agency for any specified Service Period.

4. Satisfaction Surveys

4.1 The Client may undertake satisfaction surveys in respect of the Agency's provision of the Goods or Services. The Client shall be entitled to notify the Agency of any aspects of their performance of the provision of the Goods or Services which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Order 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 His Majesty's Ships or Vessels and Service Stations;
"Officer in charge"	shall include Officers Commanding Service Stations, Ships' master's or Senior Officers, and Officers superintending Government Establishments;
"Priority 1"	Critical: Incidents falling under this category have a significant impact on business operations and require immediate attention. For example, a complete system outage affecting multiple departments.
"Priority 2"	High: Incidents in this category have a notable impact but may not be as severe as critical incidents. They require swift resolution to prevent further disruption. An example could be a software bug affecting a critical business process.
"Priority 3"	Medium: This category encompasses incidents that have a moderate impact on business operations and can be resolved within a reasonable timeframe. For instance, a single user experiencing intermittent connectivity issues.
"Priority 4"	Low: Incidents classified as low priority have a minimal impact on business operations and can be resolved without significant disruption. A minor cosmetic issue on a non-critical webpage could be an example.
"First Line"	**First line**: provides basic or common assistance, such as resetting passwords

	or troubleshooting network issues. They are usually the first point of contact for customers.
“Second Line”	**Second line**: handles more complex or technical tasks, such as installing software or configuring hardware. They may escalate issues to third line if they cannot resolve them.
“Third Line”	**Third line**: deals with external services or highly technology-specific issues, such as contacting vendors or developing custom solutions.
“Hosting environment”	The website infrastructure is hosted on MOD’s hosting infrastructure, known as MODCloud.

2 Access to MOD sites

2.1 The Client shall issue passes for those representatives of the Agency 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 Client and shall be surrendered on demand or on completion of the supply of the Goods or Services.

2.2 The Agency'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 Agency 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 Client 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 Agency'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 Agency. When sleeping accommodation and messing facilities are not available, a certificate to this effect may be required by the Client and shall be obtained by the Agency from the Officer in charge. Such certificate shall be presented to the Client with other evidence relating to the costs of this Contract.

2.4 Where the Agency'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 Agency shall make such arrangements through the Technical Branch named for this purpose in the Client Contract Details. When such transport is not available within a reasonable time, or in circumstances where the Agency wishes its representatives to accompany material for installation which it is to arrange to be delivered, the Agency shall make its own transport arrangements. The Client shall reimburse the Agency'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 Agency'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 Agency'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 Agency's representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Agency at rates fixed in accordance with current Ministry of Defence regulations.

2.6 Accidents to the Agency'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 Agency'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 Agency 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 Client shall, upon request by the Agency and subject to any limitation required by the Agency, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made at the Site to which the Agency's representatives are attached. All such advances made by the Client shall be recovered from the Agency

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 an Order 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 Order Contract and for the avoidance of doubt, award of the Order Contract by the Client 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 Agency acknowledges that any such authorisation by the Client 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
513	**04/22**	**VAT and other taxes**
522	**11/21**	**Payment and Recovery of Sums due**
531	**09/21**	**Disclosure of information**
532B	**12/22**	**Protection Of Personal Data (Where Personal Data is being processed on behalf of the Authority)**
604	**06/14**	**Progress Reports**
609	**07/21**	**Contractor's records**
642	**07/21**	**Progress Meetings**
656A	**08/16**	**Termination for Convenience – Under £5m**
658	**10/22**	**Cyber** The Cyber Risk Profile (as defined DEFSTAN 05/138) for this requirement is **Not Applicable**. The Cyber Risk Assessment Reference is RAR-719386072
660	**12/15**	**Official Sensitive Security Requirements**

Order Schedule 18 (Background Checks)

1. When you should use this Schedule

This Schedule should be used where Agency Staff must be vetted before working on the Contract.

2. Definitions

"Relevant Conviction" means any conviction listed in Annex 1 to this Schedule.

3. Relevant Convictions

3.1 The Agency must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Goods or Services without Approval.

3.2 Notwithstanding Paragraph 3.1 for each member of Agency Staff who, in providing the Goods or Services, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Client owes a special duty of care, the Agency must (and shall procure that the relevant Sub-Contractor must):

(a) carry out a check with the records held by the Department for Education (DfE);

(b) conduct thorough questioning regarding any Relevant Convictions; and

(c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Agency shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Goods or Services any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

None

Order Schedule 20 (Order Specification)

1. Introduction

A key aim of DE&S is to recruit a high-quality, highly skilled and diverse workforce to ensure that the organisation can perform to the best of its ability and deliver its OGSMs and on the aims of the DE&S strategy. The DE&S website, launched in May 2018, plays an important role in supporting this aim and in delivering strategic objectives. It also has a secondary role as a source of news and information about the work and role of DE&S helping to enhance its external reputation with potential employees and among key stakeholders. It is a much needed 'shop window' and a vital digital presence for the organisation in the digital age. Publishing for the website is done in house by the Corporate Comms team and the site is hosted on an MOD Hosting Environment (MODCloud).

The Authority are looking to put a new support contract in place to ensure continued technical support for the website covering both anticipated maintenance and unanticipated problems.

2. Technical details: hosting and tech stack

In line with government digital service best practice the website uses mainly Open-Source applications

- Built using the WordPress CMS, using a theme called Avada.
- Technology stack: standard Linux, Apache, MySQL, PHP (LAMP)
- Data (content) is no more than OFFICIAL (website is public facing).
- The website is hosted on the MODCloud ICE service
- Support will require access to the Hosting Environment and therefore personnel involved will need to have SC clearance.

3. Scope

3.1. In Scope

There is a requirement for ongoing monthly support and maintenance of the DES Website, for a period of two years. The requirement is specified in the *Requirements* section, the main support activities will be:

- Provision of ongoing monitoring, housekeeping and maintenance work on the existing web application.
- Develop an understanding of the codebase and Hosting Environment, and to take ownership of the code.
- Resolving *ad hoc* bugs and other issues that arise.
- Work with the hosting team to ensure that the application and supporting software is configured to optimise the security and integrity of the site.
- Automated monitoring of site performance for potential issues
- Ad hoc technical support for issues automatically raised or flagged via client requests.
- Liaise directly with MODCloud team to resolve issues between the applications and hosting infrastructure.

3.2. Out of Scope

- Development of a new website

- Website hosting
- Creation of new pages or content on the website
- First line support for the website
- Publishing of content.

4. IT / Information / Cyber security:

The Contractor should inform the Authority if they propose to introduce additional monitoring or other measures as part of the protection of the Confidentiality, Integrity and Availability of the DE&S website including the information contained within. Note that the website sits in a secure Hosting Environment delivered through MODCloud (Annex 1 shows a high-level diagram of the hosting infrastructure which includes end-to-end protective monitoring service provided through MODCloud.

- Confidentiality – Protection of information / data relating to Users and their accounts.
- Integrity – Protection of DE&S information and content hosted on the website.
- Availability – Protection of the availability and accessibility of the website and its content.

The Contractor should reference in their Tender response if they propose to put in place additional services to protect, prevent and/or detect any direct or indirect cyber-attacks against the DE&S website.

It is expected that the Contractor is Cyber Essentials Plus and ISO27001 compliant.

The Contractor will be expected to provide **Second** and **Third** Line of support (based on ITIL v4 model defined in Order Schedule 17)

5. Requirement

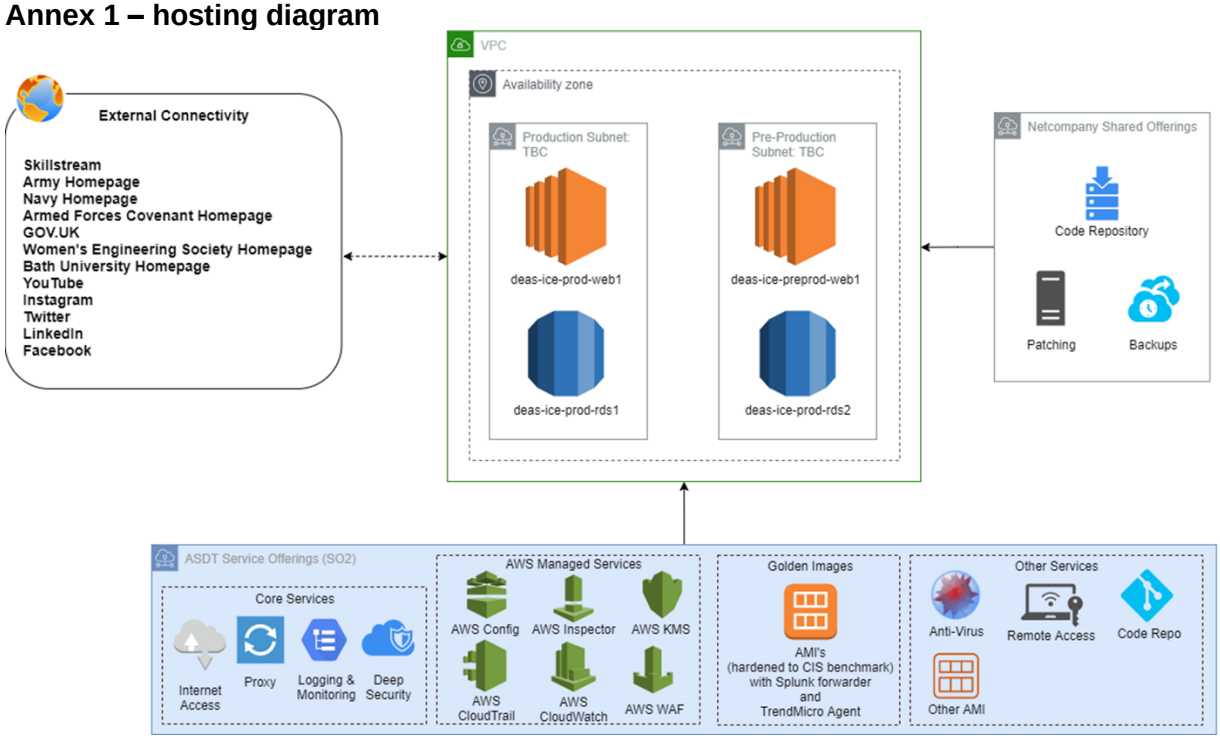
5.1. Support Service Requirement

The DES Website Service Requirement		
Serial	**Requirement**	**Critical Acceptance Criteria**
0	The Discovery Phase is an opportunity for the Contractor to undertake due diligence to understand the codebase and Hosting Environment. The winning Contractor will have a period of 5 days to conduct the Discovery Phase and a further 2 days to provide a report to the Authority.	Contractor to provide a plan including timeline for conducting the Discovery Phase. Contractor to provide a report outlining work undertaken and costs incurred against the milestone.
1	The Contractor shall provide a single point of contact (e.g. phone number, email address or web form) to raise incidents on a 24/7 basis which as a minimum allows Authorised Users to raise incidents. In addition to this and a direct way of contact, e.g. an email address, should be provided to escalate incidents of the highest priority, and in case that platform is also affected.	Technical issues logged under this facility should be acknowledged within one hour of the start of the next working day. See Order Schedule 14 Annex A
2	The Contractor shall be available to provide technical support to resolve service incidents, problems, and requests (terms as defined by	Availability of Contractor to provide technical support Monday to Friday 09:00 –

	ITIL v4) on a or 09:00-17:00 Mon – Fri basis (excluding public holidays).	17:00(excluding public holidays)
3	The Contractor shall provide Second and Third Line support for the technical application and infrastructure support. The Authority will provide First line support and triage raised issues. If unresolved these will be escalated to either MODCloud (if hosting related) or to the Contractor for resolving.	As per Second and Third line support requirements and accepted by the Project Manager
4	The Contractor shall apply Information Technology Infrastructure Library (ITIL v4) best practices, including incident, problem and change management to minimise the risk of recurring problems.	As demonstrated in performance of the requirement and accepted by the Project Manager
5	The Contractor must ensure that personnel accessing the Hosting Environment (MODCloud ICE) will need to hold valid Security Check (SC) clearance	Demonstrated by evidence that all personnel accessing the Hosting Environment hold valid SC clearance and accepted by the Project Manager
6	The Contractor shall maintain incident resolution times in accordance with the Service Level Agreement (SLA) at Order Schedule 14 (Service Levels) When the Contractor detects an incident before it has been reported by the Authority, it shall inform the Authority about incidents within 1 hour of occurrence (as defined by active monitoring or incident) with notifications delivered via email to the nominated DE&S point(s) of contact or mailbox(es).	Compliance with Schedule 14 (Service Levels) of the Order Form and via reporting against SLAs and accepted by the Project Manager All incidents to be reported within 1 hour of occurrence as per requirement and accepted by the Project Manager
7	The Contractor will use active system monitoring and alerting for service availability, infrastructure, data replication and security.	Contractor shall provide evidence of system monitoring as part of the monthly report which shall be issued to the Project Manager for acceptance.
8	The Contractor shall maintain a Business Continuity and Disaster Recovery process, and make this available for review by the Authority, in accordance with the Business Continuity and Disaster Recovery Plan on an annual basis throughout the life of the contract.	The Contractor to provide their Disaster Recovery Plan on an annual basis.
9	The Contractor shall provide an agreed technical resolution within one Working Day of the issue being raised to the helpdesk, for a Priority 1 incident (critical incident impacting on all users) or five Working Days for a Priority 3 incident (minor incident with little impact).	When issue is fixed, the Contractor must provide a report, within seven Working Days, detailing how the issue has been fixed and how the Contractor will prevent reoccurrence.
10	The Contractor will agree a schedule and install software updates and patches once released by the third-party providers.	The Contractor will provide a release and deploy schedule (usually done at quieter times

	The DE&S website service shall receive: • critical security patches within two weeks of release. • non-critical security patches at a minimum of every six months. • major functional upgrades at a minimum once per year in agreement with the Authority. • incremental upgrades as needed for fault resolution of incidents of Priority 3 and above.	to minimise disruption) to be agreed with the Project Manager. The Contractor will install patches made available publicly. If fixes are implemented the Contractor must provide documentation confirming the scope of the changes for each update, patch or bug fix to allow review by the Authority before being installed. Changes will need to be released first in a pre-production environment and when tested will then be released to the Production environment.
11	The Contractor shall make bug fixes available and notified to the Authority once released for use and installation guide to be provided.	
12	The Contractor shall make software upgrades / updates when these are made available by the third-party providers and notify the Authority once released for use and installation guide to be provided.	
13	The Contractor shall attend virtual monthly service reviews	Attendance by Suitable Qualified Experience Personnel at monthly service reviews conducted with the Authority.
14	The Contractor shall provide monthly service performance reports within ten Working Days of the end of the month.	Monthly service report agreed with the Authority. The report must contain all service performance details in accordance with Schedule 14 (Service Levels) of the Order Form - SLA and the system administration SLA.
15	The Contractor shall undertake Tasks as directed by the Authority through Schedule 25 (Tasking)	As defined in the relevant Tasking Form.

Annex 1 – hosting diagram



Order Schedule 24 (Security Aspects Letter)

Ministry of Defence

de&s

[Redacted]

[Redacted]

Date: 19/02/2024 Our Reference: 708385450

708385450 - DE&S WEBSITE SUPPORT

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.
2. Aspects that constitute OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
User Account Profile Information (Single)	OFFICIAL-SENSITIVE
User Account Profile Information (Bulk)	OFFICIAL-SENSITIVE
System Logs (incl user log ins)	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

Copy via email to:
[Redacted]

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

Purpose

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

Definitions

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

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

Security Grading

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

[Redacted]

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:

[Redacted]

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:

[Redacted]

Details of the CPA scheme are available at:
[Redacted]

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.

[Redacted]

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[1]. For the avoidance of doubt the term *"drives"* includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

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

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

Loss and Incident Reporting

29. The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or 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.

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

JSyCC WARP Contact Details
Email: [Redacted] (OFFICIAL with no NTK restrictions)
RLI Email: [Redacted] (MULTIUSER)
Telephone (Office hours): [Redacted]
JSyCC Out of hours Duty Officer: [Redacted]
Mail: [Redacted]

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:

[Redacted]

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:

[Redacted]

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:

[Redacted]

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.

Order Schedule 25 - Additional Services / Tasking Form

Price in accordance with Order Schedule 5 using the Contractor Day Rate Card Pricing Table for Taskings

TASK AUTHORISATION FORM - TAF Part 1	TAF NO:
CONTRACT No: 708385450 - DE&S Website Support	
PART 1 – TASK SPECIFICATION	
TASK TITLE:	
TASK DESCRIPTION (including activities, acceptance criteria and deliverables where appropriate):	
REQUIRED DELIVERY/COMPLETION DATE:	
Authority Project Manager (PM): Name:……Position……..Signed:……Date:……	

TASK AUTHORISATION FORM - TAF Part 2	TAF NO:
CONTRACT No:	
PART 2 – CONTRACTORS OFFER	
TASK TITLE:	

FIRM PRICE QUOTATION

The Contractor's Firm Price quotation for the above Task is £ (Ex VAT).

In accordance with DEFCON 127, the price breakdown including; Direct Labour (Man hours and Rate card rates); Materials; Sub-contracted work;

Role	Level	Days	Rate	Total

1. * Sub-Contract quotes are attached (* Delete as appropriate)
2. Include brief details of any significant items required to be purchased to complete the task.

DELIVERY/ COMPLETION DATE:
THIS QUOTATION IS VALID UNTIL (DATE):

CONTRACTORS AUTHORISING OFFICER
Name:…….. Position:……. Signed:……... Date:…….

PARTS 3 & 4 FOR AUTHORITY USE ONLY

TASK AUTHORISATION FORM - TAF Part 3	TAF NO:
CONTRACT No:	
APPROVAL TO PROCEED WITH TASK	
TASK TITLE:	
A. AUTHORITY NOMINATED REPRESENTATIVE I confirm that the direct labour hours and the material elements of the Firm Price quotation are commensurate with the work involved. Name:……..Position:…….. Signed:……..... Date:……..	
B . AUTHORITY FINANCE PROJECT APPROVAL FOR ALL TASKS I confirm that Sufficient Funds exist under the UIN/RAC/LPC and a Requirement Scrutiny has been undertaken. Name:……Position……...Signed:……..…….Date:……20	
C. AUTHORITY COMMERCIAL APPROVAL FOR ALL TASKS Required for all Tasks before commencement of work Name:…….Position…….Signed:……Date:……	
AGREED FIRM PRICE £ (Ex VAT)	
AGREED DELIVERY/COMPLETION DATE:	

Completion Certificate

TASK AUTHORISATION FORM – TAF Part 4	TAF NO:
CONTRACT No:	
CERTIFICATION OF COMPLETION OF TASK	
TASK TITLE:	

CONTRACTOR'S DECLARATION

DATE TASK COMPLETED on:

Name:……Position……..Signed:……..…….Date:……20

AUTHORITY NOMINATED REPRESENTATIVE ACCEPTANCE OF COMPLETION

I confirm that the task has been satisfactorily completed.

Name:……Position……....Signed:……..…….Date:……20