SCHEDULE 18 – ENABLING AGREEMENT FOR SOLUTION 4

ENABLING AGREEMENT

[Secretary of State for Defence (MOD)]

THIS ENABLING AGREEMENT is made the 24th day of April 2019

BETWEEN:

(1) Secretary of State for Defence (MOD); REDACTED TEXT
and

(2) Hogg Robinson Travel (Ltd) (a company registered in England, Scotland and Wales under company number 2107443 (the **"Supplier"**) whose main or registered office is at REDACTED TEXT

together referred to as the **"Parties"** and is effective as of the Commencement Date for the Enabling Agreement.

WHEREAS:

RECITALS

(A) The Customer wishes for the Supplier to provide Offline and Online Travel Solutions to the Customer under the centralised arrangements that the Enabling Authority has put in under the Commercial Agreement for purchasing such services by the Customer.

(B) The Commercial Agreement referenced in Recital A above for the Services was entered into between the Enabling Authority and the Supplier on 27th February 2018

(C) With reference to Recitals (A) and (B) above, the Customer wishes, and the Supplier has agreed to provide the Services in accordance with the terms and conditions of the Enabling Agreement.

NOW IT IS HEREBY AGREED as follows:

PART A

1A PART A PROVISIONS

1A1 Initial Enabling Agreement Period

1A1.1 The Enabling Agreement shall take effect on the Commencement Date of the Enabling Agreement 2nd May 2019 and, subject to Clause 1A1.2 below, shall continue until the end of the Initial Commercial Agreement Period of the Commercial Agreement. The Go Live Date for MoD is the 15th July 2019 and 29th July 2019 for DSTL.

1A1.2 The Enabling Agreement shall continue:

(a) until its expiry 28 February 2021;

(b) The Customer shall have the right at the end of the Initial Enabling Agreement Period to elect to extend this Enabling Agreement for one or more further periods, totalling no more than twelve (12) months in aggregate (each an "**Extension Period**") on and from the expiry of the Initial Enabling Agreement Period by giving the Supplier not less than six (6) months' written notice prior to the date of expiry of the Initial Enabling Agreement Period or the then-existing Enabling Agreement Period (if previously extended), as applicable;

(c) unless the Enabling Agreement is terminated in accordance with the terms of the Enabling Agreement provided always that such termination is escalated to the Enabling Authority and the Supplier for resolution in accordance with the Dispute Resolution Procedures in Schedule 14 (Governance) of the Commercial Agreement, as more particularly described in Clause A19.4 of the Commercial Agreement.

1A2 Beneficiaries – the Customer

1A2.1 The Supplier acknowledges and agrees that the rights and benefits of the Enabling Authority as set out in the Clauses of Part A of the Commercial Agreement, Schedule 5 (Security Requirements), Schedule 22 (Business Continuity and Disaster Recovery) and Schedule 7 (Implementation Schedule) to Schedule 17 (Exit) of the Commercial Agreement are not solely for the benefit of the Enabling Authority and will, where applicable, also be for the benefit of the Customer. Unless otherwise stated in the Enabling Agreement, the Customer will be a Third Party Beneficiary under the Commercial Agreement in respect of rights and benefits under the Clauses

of Part A of the Commercial Agreement, Schedule 5 (Security Requirement), and Schedules 7 (Implementation Schedule) to Schedule 17 (Exit), as more particularly described in Clause A6 of the Commercial Agreement.

1A3 Beneficiaries – the Enabling Authority

1A3.1 The Customer and the Supplier agree that the Enabling Authority is a beneficiary under the Enabling Agreement and has a right to enforce the relevant terms of the Enabling Agreement in accordance with Clause B35.12 of the Commercial Agreement.

1A4 Performance of the Services

1A4.1 The Supplier shall provide the Services in accordance with the terms of the Enabling Agreement, including Schedule 1 (Definitions) to Schedule 4 (Pricing and Invoicing) and Schedule 6 (Staff Transfer and Pensions).

1A5 Termination and Dispute Resolution Procedure

1A5.1 Notwithstanding any other provision of the Enabling Agreement, the Parties agree that any termination right that either the Supplier and/or a Customer may wish to exercise under the Enabling Agreement, shall be escalated to the Enabling Authority and the Supplier for resolution in accordance with Dispute Resolution Procedure in Schedule 14 (Governance) of the Commercial Agreement. The Parties agree that the relevant Enabling Agreement cannot be terminated unless and until the Dispute Resolution Procedure is followed in accordance with this Clause 1A5.1 and Clause A19.4 of the Commercial Agreement.

1A5.2 Notwithstanding any other provision of the Enabling Agreement, in respect of all Disputes between the Customer and the Supplier that are being attempted to be resolved in accordance with the terms of the Enabling Agreement, if such Dispute has not been resolved by the end of the commercial negotiation phase under Clause 1C1.6 of the Enabling Agreement, such Dispute shall be escalated to the Enabling Authority and the Supplier for resolution in accordance with Dispute Resolution Procedure in Schedule 14 (Governance). For the avoidance of doubt, the escalation pursuant to this Clause A5.2 to the Enabling Authority and the Supplier under Schedule 14 (Governance) shall commence at the level beginning at paragraph 6.1(2) of Schedule 14 (Governance).

1A6 Consent of the Enabling Authority

1A6.1 The Parties agree that any changes that need to be made to the Enabling Agreement (including prior to its execution by the Parties) shall require the prior written approval of the Enabling Authority. Such prior written approval shall be in accordance with Schedule 16 (Variation of Commercial Agreement Form). Any amendment made in the Enabling Agreement or an

attempt in the Enabling Agreement to amend the Commercial Agreement shall be void and of no effect unless such amendment has been made in accordance with this Clause A16.1.

1A6.2 The Customer and the Supplier shall inform the Enabling Authority in writing prior to entering into an Enabling Agreement. Such prior written approval shall be in accordance with Schedule 16 (Variation of Commercial Agreement Form).

1A6.3 The Customer and the Supplier shall not agree or incorporate any Special Requirements in Annex 2 (Customer Bespoke Service Requirements) without the prior written approval of the Enabling Authority. Such prior written approval shall be in accordance with Schedule 16 (Variation of Commercial Agreement Form).

1A7 Incorporation of the Clauses and Schedules of the Commercial Agreement into the Enabling Agreement

1A7.1 Part B and Part C of the Enabling Agreement sets out the terms and conditions dealing with which Clauses (or parts thereof) of the Commercial Agreement and which Schedules (or parts thereof) of the Commercial Agreement are incorporated into the Enabling Agreement

PART B

1B PART B PROVISIONS

1B1 Incorporation of the Clauses of Part B of the Commercial Agreement

1B1.1 Save as otherwise set out in Part C below, from the Commencement Date of the Enabling Agreement, the Clauses of Part B of the Commercial Agreement are incorporated into this Part B of the Enabling Agreement.

1B2 Incorporation of Schedule 1 (Definitions) to Schedule 6 (Staff Transfer and Pensions)

1B2.1 Save as otherwise set out in Part C below, from the Commencement Date of the Enabling Agreement, Schedule 1 (Definitions) to Schedule 6 (Staff Transfer and Pensions) of the Commercial Agreement are incorporated into the Enabling Agreement as Schedule 1 (Definitions) to Schedule 6 (Staff Transfer and Pensions) of the Enabling Agreement.

1B3 Clauses of Part A of the Commercial Agreement, Schedule 5 (Security Requirements) and Schedule 7 (Implementation Schedule) to Schedule 17 (Exit) of the Commercial Agreement

1B3.1 Subject to Clause A2.1 of the Enabling Agreement, the Parties acknowledge and agree that the Clauses of Part A of the Commercial Agreement, Schedule 5 (Security Requirements), and Schedule 7 (Implementation Schedule) to Schedule 17 (Exit) are not incorporated into the Enabling Agreement.

PART C

1C PART C PROVISIONS

1C1 Changes to Clauses of Part B of the Commercial Agreement

1C1.1 Unless otherwise stated in this Part C, all references to "Authority" and "Commercial Agreement" in the Clauses of Part B of the Commercial Agreement or Schedule 1 (Definitions) of the Commercial Agreement shall, as incorporated into the Enabling Agreement in accordance with the Clauses in Part B of the Enabling Agreement, are regarded as references to the "Customer" and "Enabling Agreement", respectively.

1C1.2 Unless otherwise stated in this Part C, all references to "Customer" and "Enabling Agreement" in the Clauses of Part B of the Commercial Agreement or Schedule 1 (Definitions) of the Commercial Agreement shall, as incorporated into the Enabling Agreement in accordance with the Clauses in Part B of the Enabling Agreement, are regarded as references to the "Authority" and "Commercial Agreement", respectively.

1C1.3 Unless otherwise stated in this Part C, all references to "Enabling Agreements", "any Enabling Agreements" or "an Enabling Agreement" in the Clauses of Part B of the Commercial Agreement or Schedule 1 (Definitions of the Commercial Agreement) shall, as incorporated into the Enabling Agreement in accordance with the Clauses in Part B of the Enabling Agreement, are regarded as references to the "the Enabling Agreement".

1C1.4 Unless otherwise stated in this Part C, all references to "Commencement Date" in the Clauses of Part B of the Commercial Agreement or Schedule 1 (Definitions) shall, as incorporated into the Enabling Agreement in accordance with the Clauses in Part B of the Enabling Agreement, are regarded as references to the "Commencement Date" of the Enabling Agreement.

1C1.5 For the purposes of incorporation of Clause B35.12 (a) of the Commercial Agreement into the Enabling Agreement, it shall be deemed to include the Enabling Authority as a Third Party Beneficiary in respect of Clause A3 of the Enabling Agreement.

1C1.6 The Dispute Resolution Procedure for the Enabling Agreement is the same as the Dispute Resolution Procedure set out in paragraph 6 of Schedule 14 (Governance) of the Commercial Agreement save that if the Dispute between the Customer and the Supplier is not resolved after the commercial negotiations phase described in paragraph 6.2(1) Schedule 14 (Governance), the Parties will escalate such unresolved dispute to the Enabling Authority and the Supplier for resolution under the Dispute Resolution Procedure of the Commercial Agreement in accordance with

Clause A5.2 of the Enabling Agreement and Clause A19.5 of the Commercial Agreement.

1C1.7 The following Clauses are incorporated into the Enabling Agreement in accordance with this Part C subject to the following terms:

(a) the text in Clause B1.2(a)(ix) shall be replaced with: “any reference to the Enabling Agreement includes Schedule 1 (Definitions) to Schedule 4 (Pricing and Invoicing) and Schedule 6 (Staff Transfer and Pensions);”

(b) [NOT USED]

(c) Clause B1.2(c) shall not be amended on incorporation into the Enabling Agreement;

(d) Clause B2.1 (Key Personnel) shall not be amended on incorporation into the Enabling Agreement;

(e) Clause B.2.2 (Supplier Personnel) shall not be amended on incorporation into the Enabling Agreement;

(f) Clause B6.5(a) shall not be amended on incorporation into the Enabling Agreement except that “Commercial Agreement” shall be changed to “Commercial Agreement and the Enabling Agreement”;

(g) Clause B6.5(c) shall not be amended on incorporation into the Enabling Agreement except that “Authority” shall be changed to “Authority and/or Customer”;

(h) [NOT USED]

(i) the text in Clause B7.2(d) shall be replaced with:

"The Supplier acknowledges and agrees that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the relevant Customer as a result of the Supplier's failure to meet the Service Levels in accordance with Schedule 3 (Service Levels and Service Credits)";

(j) any reference to "Management Charge" in the text in Clause B8 (Variation Procedure) shall be changed to "Charges";

(k) a new Clause B8.1(e) shall be added to Clause B8 (Variation Procedure) which states:

"notwithstanding the provisions of this Clause B8 above, any variation of the Enabling Agreement is subject to the terms of Clause A6 (Consent of the Enabling Authority) of the Enabling Agreement;"

(l) the text in Clause B17.2(k) shall not be amended on incorporation into the Enabling Agreement;

(m) Clauses B21 to B23 shall not be amended on incorporation into the Enabling Agreement;

1C2 Changes to Schedules 1 (Definitions) to Schedule 4 (Pricing & Invoicing) and Schedule 6 (Staff Transfer and Pensions)

1C2.1 For the avoidance of doubt, definitions specific to the delivery of the requirements of this enabling agreement have been included within Annex 2 – Statement of Requirements;

Signed for and on behalf of the Customer, **Ministry of Defence (MOD)**

By: ____REDACTED TEXT _____

Name: _____REDACTED TEXT_____

My position is _____REDACTED TEXT_____ and I confirm that I have authority to sign this Enabling Agreement on behalf of **Ministry of Defence (MOD)**

Date: _____17th April 2019_____

Signed for and on behalf of **Hogg Robinson Group**

By: _____ REDACTED TEXT_____

Name: _____REDACTED TEXT_____

Title: ____REDACTED TEXT_____

Date: ___2nd May 2019_____

Annex 1 – Pick List

The Customer must provide the following information to the Supplier upon signing the Enabling Agreement, to assist the successful set up and implementation of this new account for Commercial Agreement RM6016.

Customer Name: - Ministry of Defence (MOD)

Names of all Departments / Arm's Length Bodies (ALBs) etc. that will be using this Enabling Agreement:

- Head Office and Corporate Services (HOCS)
- Defence Equipment and Support (DE&S)
- Royal Air Force
- Royal Navy
- The British Army
- Joint Force Command (JFC)
- Defence Business Services (DBS)
- Defence Science and Technology Laboratories (Dstl)
- Defence Infrastructure Organisation (DIO)
- Defence Electronics and Components Agency (DECA)

Your Name: - ___ REDACTED TEXT

Key Customer Contacts for this Enabling Agreement			
Name	**Position**	**Telephone**	**Email**
REDACTED TEXT	REDACTED TEXT	REDACTED TEXT	REDACTED TEXT
REDACTED TEXT	REDACTED TEXT	REDACTED TEXT	REDACTED TEXT

REDACTED TEXT	REDACTED TEXT	REDACTED TEXT	REDACTED TEXT

The Ministry of Defence
REDACTED TEXT

Ministry of Defence
REDACTED TEXT
Dstl Accounts Payable
REDACTED TEXT

SECTION A - SERVICE REQUIREMENTS:

The Services required from Commercial Agreement Solution 4 are:-

To be bookable Online	Yes	No	Later
Rail	✓		
Air	✓		
Accommodation	✓		
Eurostar	✓		
Taxi Bookings	✓		
Ferry Bookings	✓		
Airport, train station, port parking	✓		

International Vehicle Hire (Authority approval required via RM1062)	✓		

To be bookable Offline	Yes	No	Later
Rail	✓		
Air	✓		
Accommodation	✓		
Eurostar	✓		
Le Shuttle (Euro Tunnel)	✓		
Group accommodation	✓		
Long stay accommodation	✓		
International Vehicle Hire (Authority approval required) (via RM1062)	✓		
Airport, train station, port parking	✓		
Group Booking Service (with individual PNR)	✓		
Group Booking Service (without individual PNR)	✓		
Season Tickets	✓		
Transport for London bookings (including Oyster cards)	✓		
Rail warrant bookings	✓		

Book for third party travellers	✓		
Visa, passport	✓		
Meet and Greet Service		✓	
Coach or bus tickets	✓		
Coach hire with driver	✓		
Ferry Bookings	✓		
Taxi Bookings	✓		
Executive Services		✓	
Air charter		✓	
Special assistance for exceptional circumstances, e.g. escorted travellers, unaccompanied minors or an accompanied traveller service requirement for visually impaired travellers	✓		
Travel Service Implants		✓	
Additional Requirements as per paragraph 17 of Schedule 2 (please specify below) detailed in Annex 2 and Annex 2a	✓		
Any other services: ● As detailed in Annex 2 and Annex 2a	✓		

Insert here any <u>non-mandatory</u> online and/or offline requirements from Schedule 2 as well as any requirements under Paragraph 17 of Schedule 2 which you would like to discuss with the Supplier during Implementation:

Non-mandatory requirements detailed in Appendix B	
N/A	

SECTION B – PAYMENT OPTIONS REQUIREMENTS:

Pricing Option	✓ A – Booking Service Fee Model ❑ B – Commissions Share Model ❑ A and C – Booking Service Fee Model and Implant Services ❑ B and C – Commissions Share Model and Implant Services
Payment Options :	✓ Corporate payment cards ✓ Billing to project and or cost centre ✓ Lodge cards / enhanced lodge cards ✓ Individual and / or single bill back, for example non-consolidated invoices ✓ Payment on departure by Traveller for accommodation bookings Consolidated invoice accounts, for example 10 or 30 days
Invoicing Options :	❑ N/A ❑ Weekly Consolidated Invoice - 10 Day Settlement Terms ✓ Weekly Consolidated Invoice - 30 Day Settlement Terms ❑ Fortnightly Consolidated Invoice - 10 Day Settlement Terms ❑ Fortnightly Consolidated Invoice - 30 Day Settlement Terms ❑ Monthly Consolidated Invoice - 10 Day Settlement Terms Monthly Consolidated Invoice - 30 Day Settlement Terms

	Other
Returned Commissions:	N/A

SECTION C - TRAVEL POLICY & PROCESS REQUIREMENTS:

The Customer must provide contact details of the individual/s that are to receive the agreed invoice (if applicable). The Supplier shall email all invoices. Please complete the table below.

Email Address	**Finance Contact Name**	**Telephone Number**
REDACTED TEXT	**TBC**	**TBC**
REDACTED TEXT	REDACTED TEXT	
REDACTED TEXT	**TBC**	**TBC**

The Customer must list all mandatory cost codes, purchase order numbers or any other codes that need capturing: **Please complete the table below.**

Code Fields title: (e.g. Cost Centre, PO Number etc.)	**Mandatory Field: (Yes/No)**	**Format: (e.g. Validation table, Mask, Drop down). **Please also provide any list of codes.***	**Shown on Invoice ?**	**Additional comments:**
Separate Attachment		Unique Identification Numbers (UINs) REDACTED TEXT by DBS Liverpool		
Vendor Agreement Number	Y	Table	Y	
Dstl Cost Centre	Y	REDACTED TEXT	Y	
DSTL Project Codes	Y	REDACTED TEXT	Y	

Online Booking System Policy Configuration and Offline Service(s) Access	Customer Response
Do you have any other reason codes than listed in Schedule 2?	No
If Yes, please specify:	N/A
Do you have any policies on class of rail travel?	Yes
If Yes, please specify:	MOD Business Travel Guide & JSP 800 Vol 2. Dstl Travel Policy Guide See Annex C, D and E of the ITT.
Do you have a preferred default method for rail ticket fulfilment?	Yes
If Yes, please specify:	✓ Customer onsite Printer (own) ✓ Customer onsite Printer (New/Suppliers) ✓ Ticket on Departure ✓ First Class Post ✓ Second Class Post ✓ Print at Home/Self Print ✓ Collection at Station Window ✓ Recorded or Special Delivery Post Courier Service ✓ Smartcard / Bar Code / Smart Phone Application ✓ Travel Card/Rail Card I.e. Senior Citizen but NOT HM Forces

	✓ Seating preferences
Do you wish to purchase or lease desktop or kiosk printers?	Yes
If Yes, please specify: i.e. The number, type, whether purchases or leased and location of the printers.	Yes See Annex F
Do you require maintenance contracts associated with either purchased, leased or Customer Owned ticket printers?	Yes
If Yes, please specify:	REDACTED TEXT
Do you have any policies on class of air travel?	Yes See Annex C of the ITT.
If Yes, please specify: e.g. do not display / provide first class air fares	MOD Business Travel Guide & JSP 800 Vol 2. Dstl Travel Policy Guide See Annex C, D and E of the ITT.

Do you have any policies on flight duration? If Yes, please specify below*	Yes (See above)
Do you have any policies on accommodation? If Yes, please specify below**	Yes See Annex C and D of the ITT- MOD & Dstl Business Travel Guide
Do you want the Supplier to operate a rate cap management policy? ***	Yes
If Yes, please specify:	The capture of all over cap expenditure and the reasons why adjust rates if appropriate Monitor of all rates ensuring that they are at set at the minimum possible whilst still ensuring sufficient available bed stock Introduce a monthly policy of sample and review Content for colour coding, as suggested below, but not a block on booking.
Do you require the exclusion of sale of certain routes or airlines? Locations or accommodation providers?	Yes
If Yes, please explain the reasons behind such exclusion:	Please refer to**: Regulation (EU) 2017/2215 of 30 November 2017.** **Link below** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2215
Do you require pre-trip authorisation?	Yes

If Yes, please specify:	REDACTED TEXT
Do you require a bespoke automated attendant model and/or interactive voice response telephone script?	Review at implementation stage
If Yes, please specify:	
Do you require the facility to book valuable or sensitive items on flight or rail bookings?	Yes
If Yes, please specify:	REDACTED TEXT
Do you require the facility for offline bookings to be made without the need to create or store permanent traveller profile?	Yes
If Yes, please specify:	Contactors without staff numbers, families, recruits
Have you provided a copy of your Travel Policy?	Yes
Do you need to update the list of cost centre codes, employee numbers, GL strings, Project Codes or WPS numbers more than 12 times per year?.	Yes
Any other policy requirements? If Yes, please specify:	Additional policy requirements contained in travel policy documents at Annex C, D and E of the ITT.

Any other special booking requirements? If Yes, please specify:	Please refer to Appendix B Statement of Requirements

Flight Duration Policy*

Flight Duration Policy* - Dstl

Flight Duration in hours	Class of Travel Permitted	Comments:
Up to 4 hours	**Economy**	**+/- 2 hours of requested arrival time**
Between 4 and 10 hours	**Premium economy or equivalent**	**+/- 4 hours of requested arrival time**
More than 10 hours	**Business or equivalent**	**+/- 4 hours of requested arrival time**

Accommodation Spend Limits**

Location:	Accommodation cap/Amber Policy	Cut off cap/Red Policy (if applicable)	Comments:
London	£	£	Refer to MOD Rate Caps at Annex 2- Customer Bespoke Service Requirements
Outside of London	£	£	Refer to MOD Rate Caps at Annex 2- Customer Bespoke Service Requirements

Other major cities (up to 5)	£	£	Refer to MOD Rate Caps at Annex 2- Customer Bespoke Service Requirements

Accommodation Spend Limits**

Accommodation Limits Dstl**

The following standard of accommodation is acceptable:

 Rate cap for minimum of REDACTED TEXT worldwide

Hotel to a 3 star or equivalent standard

 Adequate safety and personal security standards

 Single room occupancy

 En-suite facilities

 Tea / coffee making facilities

 Desk and space to work

 Colour television

 Telephone

Rate Cap Management Policy***

An example policy may be to use a Green, Amber and Red approach as above. Please note use of a Red policy may restrict people booking hotels when prices fluctuate.

1. Green – Anything under the hotel policy cap is within policy and can be booked
2. Red – Anything over the hotel policy cap can be booked, but the booker will have to provide a reason code to explain why they are booking over an agreed rate.

ANNEX 2 – Customer Bespoke Service Requirements

REDACTED TEXT

Hotel Capped Rates for MOD excluding Dstl:

REDACTED TEXT

- Cap Rates include the cost of breakfast and Tax
- Staff may book accommodation in any establishment, regardless of star rating, up to the capitation rate for the area
- If a hotel is required above the cap rate local budgetary approval will be required

London by Postcode

All London Postcodes are covered by the London Generic Rate of REDACTED TEXT, with the exception of:

REDACTED TEXT

Overseas

Areas which do not have their own Cap Rate are covered by the Overseas Generic rate of £REDACTED TEXT equivalent in local currency

REDACTED TEXT

MOD Specific Defcons:

Contract Change Control Procedure

1. Customer Changes
Subject always to Part B of the Enabling Agreement, the Customer shall be entitled, acting reasonably, to require changes to the Supplier Deliverables and associated obligations (a " Change") in accordance with this Condition.

2. Notice of Change
a. If the Customer requires a Change, it shall serve a Notice (an "Customer Notice of Change") on the Supplier.
b. The Customer Notice of Change shall set out the change required to the Supplier Deliverables and associated obligations in sufficient detail to enable the Supplier to provide a written proposal (a "Supplier Change Proposal") in accordance with Clause 3 below.

3. Supplier Change Proposal

a. As soon as practicable, and in any event within fifteen (15) Business Days (or such other period as the Parties may agree) after having received the Customer Notice of Change, the Supplier shall deliver to the Customer a Supplier Change Proposal.
b. The Supplier Change Proposal shall include:
(1) the effect of the Change on the Supplier obligations under the Contract;
(2) a detailed breakdown of any costs which result from the Change;
(3) the programme for implementing the Change;
(4) any amendment required to this Contract as a result of the Change, including, where appropriate, to the Contract Price; and
(5) such other information as the Customer may reasonably require.

c. The price for any Change shall be based on the prices (including all rates) already agreed for the Contract and shall include, without double recovery, only such charges that are fairly and properly attributable to the Change.

4. Supplier Change Proposal – Process and Implementation
a. As soon as practicable after the Customer receives a Supplier Change Proposal, the Customer shall:
(1) Evaluate the Supplier Change Proposal;
(2) Where necessary, discuss with the Supplier any issues arising and following such discussions the Customer may modify the Customer Notice of Change and the Supplier shall as soon as practicable, and in any event not more than ten (10) Business Days (or such other period as the Parties may agree) after receipt of such modification, submit an amended Supplier Change Proposal.

b. As soon as practicable after the Customer has evaluated the Supplier Change Proposal (amended as necessary) the Customer shall:
(1) Indicate its acceptance of the Supplier Change Proposal by issuing a serially numbered amendment letter in accordance with Condition B8 of the Commercial Agreement, and Part B of the Enabling Agreement; or
(2) Serve a Notice on the Supplier rejecting the Supplier Change Proposal and withdrawing (where issued) the Customer Notice of Change.

c. If the Customer rejects the Change Proposal it shall not be obliged to give its reasons for such rejection.
d. The Customer shall not be liable to the Supplier for any additional work undertaken or expense incurred unless a Supplier Change Proposal has been accepted in accordance with Clause 4.b.(1) above.

5. Supplier Changes
If the Supplier wishes to propose a Change, it shall serve a Supplier Change Proposal on the Customer, which shall include all of the information required by Clause 3.b above, and the process at Clause 4 above shall apply.

Unlimited Liability

In accordance with B19 of the Commercial Agreement the Supplier shall not limit it's liability under any circumstances under this Enabling agreement.

ANNEX 2a – Specification of Requirements, tenders for Further Competition

1. Definitions

Expression or Acronym	Definition
API	means Application Programme Interface
Authority	means Crown Commercial service as defined in the Commercial Agreement
BDS	means British Defence Staff
Booker	means an employee, agent or representative of the Customer who wishes to make a booking via online or offline methods;
Crisis Management	means the process by which the Supplier deals with a sudden emergency situation; where Crisis is referred and incidents this shall apply.
CTVS	means Crown Travel and Venue Services
Customer(s)	means Ministry of Defence including Dstl and its executive agencies
DfT	means Department for Transport
DFID	means Department for International Development
DILFOR	REDACTED TEXT
Dstl	means Defence Science and Technology Laboratories
FCO	means Foreign Commonwealth Office
FOC	means Free of Charge
FOI	means Freedom of Information
GDS	means Global Distribution System
GSC	means Government Security Classification
ICO	means Information Commissioners Office
Lodged Cards	means a centralised payment means dedicated to air and rail ticket purchases
REDACTED TEXT	REDACTED TEXT

REDACTED TEXT	REDACTED TEXT
MOD	means Ministry of Defence including Dstl and its executive agencies
TMC	means Travel Management Company
Traveller	means an employee, agent or representative of the Customer who is or will be, named on the booking as the person travelling or using the Services;
PCI DSS	means The Payment Card Industry Data Security Standard
POD	means pay on departure
UIN	means Unit Identity Number

2. PURPOSE

2.1 The Ministry of Defence (MOD), including its executive agencies and contractors, requires a travel management solution for its personnel to book train, air, ferries, taxis (Defence Science and Technology Laboratory (Dstl) only), Coaches (Dstl only) parking services, Eurotunnel, accommodation, and other ancillary services related with transportation and accommodation, online and offline to enable crown business around the world 24 hours a day, 7 days a week, 365 days a year (366 days if in a leap year). This is a fundamental enabler of core MOD business.

2.2 The MOD seeks to appoint a single Supplier to provide a fully managed end to end Travel Management solution as described in this Appendix B Statement of Requirements.

2.3 The enabling agreement duration is for two (2) years with an option to extend by one (1) year. (2+1)

2.4 The Commercial Agreement expires in February 2021, CCS will advise Customers if an option to extend the Commercial Agreement will be invoked. The Customer can not extend the Enabling Agreement beyond the term of the Commercial Agreement unless notified by CCS. There is a Termination assistance period of a further 12 months if required.

2.5 MOD will hereafter be referred to as the Customer. The resultant Enabling Agreement shall be between a single successful Supplier and the Customer and not with the Authority.

2.6 Crown Commercial Service (CCS) (hereinafter referred to as the "Authority") will manage and facilitate the procurement on behalf of the Customer.

2.7 The Enabling Agreement shall take precedence over the Commercial Agreement for the duration of this agreement. The terms within the Commercial Agreement shall apply accordingly with additional conditions and amended clauses applied within the Enabling Agreement.

3. BACKGROUND TO THE Customer

3.1 The MOD, is a central government department responsible for implementing the defence policy set by Her Majesty's Government. The department employs more than 250,000 staff which is a mix of civilian and military personnel deployed around the globe. The department is composed of multiple business areas that each have a different level of travel usage and online adoption.

3.2 The key business areas are:

- Head Office and Corporate Services (HOCS)
- Defence Equipment and Support (DE&S)
- Royal Air Force (RAF)
- Royal Navy

- The British Army
- Joint Force Command (JFC)
- Defence Business Services (DBS)
- Defence Science and Technology Laboratories (Dstl)
- Defence Infrastructure Organisation (DIO)
- Defence Electronics and Components Agency (DECA)

3.3 More information on the Customer is available from the following link:

https://www.gov.uk/government/organisations/ministry-of-defence

4. Background to requirement/OVERVIEW of requirement

4.1 The Customer currently has a travel management solution provided under the Crown Commercial Service (CCS) Crown Travel and Venue Services (CTVS) framework RM3735. This framework provides online and offline booking ability for Air, Rail, Hotels and International Car Hire. The CTVS contract end date is 19 August 2018. A 12-month transition phase has been invoked to support the procurement of travel services under a new contract up to 18 August 2019. Following an options assessment to determine the optimum value for money travel solution, the services of a Travel Management Company (TMC) is required to provide the majority of the Customer's travel needs. The Customer wishes to utilise the buying power of the TMC and the cost efficiency programmes that TMC's offer.

4.2 The Supplier shall provide efficient booking solutions that deliver value for money for the department and the public tax payer, including the ability to book unusual and complex travel needs,

4.3 Such needs might include, but not be limited to;

4.4 Facilitating routine and ad-hoc military manoeuvres such as military unit rotations and base moves around the globe. Travel needs for such requirements might include movement of hundreds of military and civilian personnel, their families, pets and equipment (such as band, medical equipment and luggage) The Supplier will be required to support these large booking requests which include all their travel requirements.

4.5 The nature of the Customer's business means personnel can be sent to locations all over the world with a day or less notice, therefore it is critical that the Supplier facilitates travel content from a variety of sources to provide cost effective fares to as many locations as possible around the globe.

4.6 Unique to the Customer is the need to provide travel around the world to a large number of recruits routinely who will not have a travel profile, and therefore no name or staff number on record. Further details are at section 7 below.

4.7 The Supplier shall deliver an offline service that must be able to accommodate complex travel needs within 5 working days' notice, or sooner where the Supplier is able. Complex travel can include large group bookings for historic visits, ski trips, training events and/or multi model and sector travel.

4.8 Defence Science and Technology Laboratories (Dstl) travel needs are part of the Customer's travel requirement for the first time. As a previous agency of the MOD, Dstl have differing requirements and the Supplier shall present the most cost-effective solution to meet both sets of requirements.

4.9 The Customer is under increasing pressure to reduce its high travel spend, and is continuously under scrutiny in the way it conducts travel, internally and externally due to the large user base, high percentage of executives, and affluent areas its personnel visits. Therefore, the Supplier shall be required to support the Customer in Freedom of Information (FOI) requests, Parliamentary questions, and detailed Management Information (MI) reporting to track and analyse travel spend. The Supplier shall support the Customer to ensure their users adhere to the travel policy in place. The Supplier shall also be required to innovate throughout the contract to reduce travel spend and improve the customer experience.

4.10 Due to the nature of the Customer's business the Supplier shall be required to obtain security clearances for some of their staff, and work with the Customer to ensure the protection of the user's data is secure. Special booking arrangements will need to be put in place to service areas of the Customer that would be unusual in the commercial sector. Further information on the security clearance required and special booking arrangement is included in the security requirements below (See Paragraph 19).

4.11 The Supplier shall be aware that the contents of this Appendix B Statement of Requirements, excludes the critical movement of units from Germany and Cyprus to the UK during 1st June – 31st September 2019 where movement of circa 11,500 personnel and families will occur. Any unit move after this timeframe, and routine travel to and from Germany and Cyprus within this timeframe remains in scope of this contract.

5. Customer IT system

REDACTED TEXT

5.1 Additionally, the Information and Communications Technology (ICT) elements of the service and systems shall throughout their life cycle, be proportionate to their functionality, data and operational maturity to ensure:

5.3.1. Compliance with the latest versions of Defence (ICT), Security, Information and Architecture Policies, Standards and Procedures, including but not limited to Joint Service Publication (JSP) 440 and JSP 604.

5.3.2. Compliance with the latest UK National and Government ICT, Security, Information, Legislation, Regulations, Good Practice Guides, Standards and Policies.

5.2 Demonstration of compliance and conformance will be through the Defence Assurance and Information Security (DAIS) Accreditation process, as the Defence Authority for Information Security and Assurance. The successful supplier will be required to work with DAIS and the Security Assurance Co-ordinator (SAC) to obtain Accreditation.

5.3 The Supplier shall apply Industry Security Notice (ISN) 2017/01 requirements to every industry owned IT and communication system used to store, process or generate MOD information including those systems containing OFFICIAL and/or OFFICIAL-SENSITIVE information. ISN 2017/01 details Defence Assurance and Risk Tool (DART) registration, IT security accreditation processes, risk assessment and risk management requirements. The ISN is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/594320/DART_ISN_-_V2_3.pdf

5.4 REDACTED TEXT

6. Applicability of Transfer of Undertakings (Protection of Employment) (TUPE)

6.1 Applicability of TUPE

6.1.1 Your attention is drawn to the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE), as amended and /or the Service Provision Change (Protection of Employment) Regulations (Northern Ireland) 2006, as amended from time to time. The Customer would be neither transferor nor transferee of the employees in the circumstances of any contract awarded as a result of this invitation and it is your responsibility to consider whether or not TUPE applies to this re-let and to tender accordingly.

6.2 **TUPE Information Provided for Tendering Purposes**

6.2.1 TUPE information in respect of the current employees is provided at Annex A. This information may be updated prior to contract award in which event the short-listed tenderers will be given an opportunity to revise or confirm submitted TUPE prices only.

6.2.2 The information detailed at Annex A has been obtained from the contractor currently undertaking this task. The accuracy and completeness of this information cannot be warranted by the Customer. It remains your responsibility to ensure that your tender takes full account of all the relevant circumstances of this contract re-let and tender accordingly. You are required to confirm when responding that you

will not make any claim or demand or take any actions or proceedings against the Customer (nor seek to avoid any contract or seek any amendment to a contract placed with the contractor by the Customer) arising from or relating to the provision of the information, whether or not you are awarded a contract as a result of this Invitation to Tender. Failure to provide clear and unequivocal confirmation may result in your tender being deemed non-compliant.

7. The requirement

7.1 The Customer requires a travel management solution for its personnel to book train, air, ferries, taxi REDACTED TEXT, Coaches REDACTED TEXT, parking services, Eurotunnel, accommodation, and other ancillary services related with transportation and accommodation, online and offline to enable crown business around the world 24 hours a day, 7 days a week, 365 days a year (366 in a leap year).

7.2 The scope of the requirement shall include all mandatory requirements in Schedule 2 Part B of the PSTVS Commercial Agreement.

7.3 The Supplier shall deliver all components as detailed in Schedule 2 Part B and as detailed within Section 7 of this Appendix B Statement of Requirements.

7.4 The Customer requires Additional Requirements to be delivered as part of this Agreement which shall also include non-mandatory requirements as detailed in Schedule 2 Part B of the PSTVS specification. Additionally, MOD specific requirements are included which are unique to this contract.

7.5 **ONLINE BOOKING SYSTEM;**

7.5.1 The following non-mandatory requirements in Schedule 2 Part B of the PSTVS are mandatory in this enabling agreement.

7.5.1.1 The Online Booking System shall provide access to an air, rail and accommodation feedback facility. The feedback facility must request the user's email address as a minimum so as to identify the provider of the feedback, and where possible, the feedback must be linked to a genuine booking made by the traveller providing the feedback.

7.5.1.2 The Online Booking System shall provide a facility for Bookers/Travellers to provide feedback on the quality of the booking system or service and third-party supplier performance and quality. The Supplier shall review this feedback as part of account management and to provide recommendations to remedy these and avoid issues occurring again.

7.5.1.3 The Supplier shall provide, within the Online Booking System a facility for the Booker and/or the Traveller to register complaints.

7.5.2 The following additional requirements in Schedule 2 Part B of the PSTVS are in scope.

7.5.2.1 The Supplier shall, book business travel for Third Party Travellers whose travel needs are associated with the business requirements of the Customer. This may include, but not be limited to, occasions where booking is required for Contractor's seconded on MOD business for a temporary period. Where bookings are made in this instance, all Travel policies will apply.

7.5.3 The following requirements are MOD specific and in addition to Schedule 2 Part B of PSTVS.

7.5.3.1 The Supplier shall make the facility available to change the booking ability of individual users (e.g. to provide the users the ability to book business class tickets when they are otherwise unavailable to the normal user). The process for controlling this ability will be agreed at the Implementation stage and will be in line with MOD Policy.

7.5.3.2 The Supplier shall provide the facility to customize the booking experience for each business area. The nature of the customisation will be agreed during implementation, but unique changes could include, limited hotel choices, differing policy thresholds, and unique fields for management information. The supplier shall allow for further customisation of the booking tool, to satisfy any changes to any of the business unit's (as listed out on Page 2 of this document) travel policy, during the course of the contract, up to four times a year, free of charge.

7.5.3.3 REDACTED TEXT

7.5.3.4 REDACTED TEXT

7.5.3.5 REDACTED TEXT

7.5.3.6 REDACTED TEXT

7.5.3.7 REDACTED TEXT

7.5.3.8 REDACTED TEXT

7.5.3.9 The Supplier shall provide an interactive map as an alternative to the list view when the user wishes to select hotels.

7.5.3.10 The Supplier's portal shall be suitable for use on multiple different computer operating systems simultaneously and be able to sustain the number of online bookings detailed in Appendix E.

7.5.3.11 The Supplier shall remove all complete itineraries from the bookers profile 24 hours after the trip is complete.

7.5.3.12 The Supplier shall make available on the online portal, content from multiple sources such as, but not limited to, Global Distribution System (GDS's), Application Programme Interfaces and rates retrieved by booking

sites and offer said rates ensuring that the lowest available fare in the market is always presented to the Booker/Traveller.

7.5.4 Desirable Requirements

7.5.4.1 The following requirements, although not mandatory to guarantee a Successful Bid, have been identified as desirable for the Customer as part of this Appendix B Statement of Requirements.

7.5.4.2 The Online Booking System should display fares/rates and availability on the day before and the day after the dates selected by the Booker.

7.5.4.3 The Online Booking System options shall be shown on a single screen, with price comparisons between travel modes, for example appropriate rail and air journeys, and should it become available during the term of the Commercial Agreement, whole journey costs.

7.5.4.4 The Supplier shall notify the Booker where there are taxi-sharing opportunities at the time of booking to assist with best value for money decisions.

7.5.4.5 The Supplier's portal shall provide a map of the London underground tube system when users attempt to book a London underground train ticket. This is to inform the Traveller's decision on which underground zone they need to book.

7.5.4.6 The Supplier shall provide, as part of the offline service, a facility to amend the traveller name whilst keeping the original booking for Rail and Hotel bookings.

7.6 OFFLINE SERVICE ACCESS & CAPABILITY

7.6.1 The following additional requirements in Schedule 2 Part B of the PSTVS are mandatory in this Enabling Agreement.

7.6.1.1 REDACTED TEXT

7.6.1.2 The Supplier shall, as part of the offline service be prepared to contact third party suppliers to fulfil specific requirements for example, staff travelling with working dogs.

7.6.1.3 The Supplier shall provide an offline facility to service long stay bookings. A long stay booking is a booking for Travellers staying more than nine (9) consecutive nights in the same accommodation.

7.6.2 The following requirements are MOD specific and in addition to Schedule 2 Part B of PSTVS.

7.6.2.1 REDACTED TEXT

7.6.2.2 REDACTED TEXT. Unique to this requirement the Supplier shall provide the option for coaches, ski passes and ski equipment, to be booked offline for the group booking.

7.6.2.3 The Supplier shall provide a service to book REDACTED TEXT, musical instruments and animals on flight or rail bookings. The Supplier shall advise of the best method of doing this, for example the need to book an additional seat, or to book the item as increased baggage allowance.

7.7 AIR REQUIREMENTS

7.7.1 The following requirements are MOD specific and in addition to Schedule 2 Part B of PSTVS.

7.7.1.1 The Supplier shall manage, on the Customer's behalf, the REDACTED TEXT, holding the redemption funds gained from qualifying flights in the suppliers account. Details of how this is to be managed is to be agreed during the Implementation stage. Further information can be found on the below websites:

REDACTED TEXT

7.7.1.2 The Supplier shall provide access and booking capabilities to Marine fares when utilization is allowed by the Airline Carrier. Further details on this shall be provided at Implementation stage.

7.7.1.3 The Supplier shall provide access and booking capabilities to Charity fares when utilization is allowed by the Airline Carrier. Further details on this shall be provided at Implementation stage.

7.7.1.4 The Supplier shall work with the Authority and the Airline Carrier to implement specific procedures on behalf of the Customer, if the Airline Carrier accept it, when the Customer requirements don't follow under the Airline Carrier standard T&C's, (eg Air Group booking with BA, additional luggage cost to be pre-paid by the Supplier and not by the traveller)

7.8 RAIL REQUIREMENTS

7.8.1 The following non-mandatory requirements in Schedule 2 Part B of the PSTVS are mandatory for this Enabling Agreement

7.8.1.1 The Supplier shall provide a process for the Customer to claim for delays to train journeys via the Supplier, where this is available. This process is to be agreed between the Customer and Supplier in the Customer Enabling Agreement, and the Supplier shall work with any third-party provider to achieve this as requested by the Customer.

7.8.1.2 The Supplier shall, provide a facility for the provision of Oyster Cards and the facility to 'top up' Oyster Cards by registering the card on the Supplier's web site or through a link to the TFL Website to allow the 'top up' to be billed back to the Customer. The use of this facility is to be agreed during the implementation stage

7.8.2 The following requirements are MOD specific and in addition to Schedule 2 Part B of PSTVS.

7.8.2.1 The Supplier shall provide a split ticketing functionality when booking rail tickets online to book cheaper fares on the routes dictated by the Customer. The split ticketing option shall be the default booking option where a saving can be made over standard or advanced tickets. The split ticketing routes will be agreed during implementation and updated if necessary following regular business reviews.

7.8.2.2 The Supplier shall process rail warrants on behalf of the Customer when the request relates to season tickets. The process for receiving rail warrant requests and sending them in the post will be agreed during the implementation stage.

7.8.2.3 The Supplier shall provide an offline service to book passenger vehicles on the Eurotunnel Le Shuttle service for business travel only (i.e. not for operational or leave travel needs).

7.8.2.4 The Supplier shall book rail travel for recruits who do not have a travel profile. This type of booking is often done in bulk (for 10 or more recruits) and occurs throughout the year to the region of 50,000 recruits or more. The Supplier shall identify the most cost-effective way of doing this, and will consider suitable saving initiatives around this requirement. The booking form (usually completed by a Business area travel cell) will be agreed during the Implementation stage.

7.9 ACCOMMODATION REQUIREMENTS

7.9.1 The following non-mandatory requirements in Schedule 2 Part B of the PSTVS are mandatory for this Enabling Agreement

7.9.1.1 For accommodation only, the results of the search shall provide maps and directions which display the distance, depending on the search criteria and mode of transport (for example, driving, walking, near rail and / or tube station).

7.9.1.2 The Supplier shall provide the Booker(s)/Travellers with the ability to detail where applicable special requirements (ie Allergies/dietary needs) on the booking tool to enable ease of travel.

7.10 PARKING REQUIREMENTS

7.10.1 The following requirements are MOD specific and in addition to Schedule 2 Part B of PSTVS.

7.10.1.1 The Supplier shall provide an online and offline facility to book parking requirements at airports, railway stations and ferry ports, which must include detailed booking information, including, but not limited to, directions and contact details for each car park reservation.

7.11 FERRY REQUIREMENTS

7.11.1 The following additional requirements in Schedule 2 Part B of the PSTVS are mandatory for this enabling agreement.

7.11.1.1 The Supplier shall provide the facility for the Customer(s) to book all ferry tickets types for domestic and international scheduled services online and offline for business travel only (i.e. not for operational or leave travel needs).

7.12 TICKET PRINTERS

7.12.1 The following non-mandatory requirements in Schedule 2 Part B of the PSTVS are in scope

7.12.1.1 The Supplier shall complete Appendix E to provide information as requested related to the FOC printers to be provided under this arrangement. The number of FOC printers must also include FOC installation, FOC service and repair, maintenance contracts and FOC training. Any ticket printer software updates required (not including Customer's system software) shall be provided FOC.

7.12.2 The following requirements are MOD specific and in addition to Schedule 2 Part B of PSTVS

7.12.2.1 Due to the Department for Transport (DfT) Smart ticket review, the Customer will seek to reduce its use of Ticket Printers over time. The Supplier shall provide prices for one (1) full year of printers, as well as option periods of six (6) month intervals until the end of the contract.

7.12.3 It should be noted that printers for MOD shall be in place by 1st April 2019.

7.13 REDACTED TEXT REQUIREMENTS

7.13.1 The following requirements are specific to REDACTED TEXT. The Supplier shall be required to work with separate REDACTED TEXT representatives during, and after, the implementation stage to ensure the following requirements are implemented:

7.13.1.1 The Supplier shall produce a Crisis Management report to be sent to a pre-defined email address as soon as possible after an event has occurred.

7.13.1.2 The Crisis management process, which will be agreed at implementation stage, will include contacting the travellers direct and reporting back to REDACTED TEXT if this is unsuccessful.

7.13.1.3 The Supplier's Named Account Manager shall attend monthly meetings with REDACTED TEXT during the implementation stage to aid set up.

7.13.1.4 The Supplier's Named Account Manager shall also attend ad hoc meetings with REDACTED TEXT post implementation stage when requested by the REDACTED TEXT travel manager.

7.13.1.5 The Supplier shall submit weekly consolidated invoicing with 30-day payment terms, and this shall be done by utilising a REDACTED TEXT. Invoice is to be provided at line detail in REDACTED TEXT to be agreed during implementation

7.13.1.6 For train journeys, the Supplier shall **not** make postal options available to the user.

7.13.1.7 The Supplier shall provide to REDACTED TEXT the ability to enter one of over 20,000 REDACTED TEXT codes that the online booking tool must validate before a booking is placed. The process to upload and amend these codes will be agreed at the implementation stage.

7.13.1.8 The Supplier shall provide, and manage, a virtual credit card solution for REDACTED TEXT l for UK use only. Payment will be made via weekly consolidated invoicing as detailed above.

7.13.1.9 The Supplier shall, provide the ability for REDACTED TEXT to make vehicle hire bookings online and offline where the point of collection and return of the vehicle is outside the UK using REDACTED TEXT.

7.13.1.10 The Supplier shall ensure that the printer maintenance contracts for REDACTED TEXT, currently provided by the extant contractor REDACTED TEXT, are replaced to ensure a continued service. The Customer shall support the Supplier where novation of contracts need to apply, this will be decided upon award of the Enabling Agreement. Further details about REDACTED TEXT printers are at Appendix C (Enabling Agreement).

7.13.1.11 The Supplier shall for REDACTED TEXT only, provide a service for the facilitation and/or processing and submission of travel visas and passports, including a visa and or passport query(s) and or support service.

7.13.1.12 The Supplier shall provide the facility to make minicab car / taxi bookings for a single Traveller or multiple Travellers online and offline and to book tickets for scheduled coach journeys, for example on intercity coach journeys, and hire a coach with a driver, online and offline, UK and abroad, for REDACTED TEXT only. The process will be agreed with the Customer(s) at Implementation and Go live stage

7.13.1.12.1 The Supplier shall take overall responsibility for ensuring that all third party providers that they engaged under this Enabling Agreement are compliant with the current and future legislation applicable to all Services, including, but not limited to, coach hire, minicab/taxi booking services and driver services.

7.14 REDACTED TEXT

7.14.1 The following requirements are specific to REDACTED TEXT only. The Supplier shall be required to work with separate REDACTED TEXT representatives during, and after, the implementation stage to ensure these requirements are implemented:

7.14.1.1 The Supplier shall provide a booking website that allows the REDACTED TEXT personnel to:

7.14.1.1.1 Use the booking portal while in the US

7.14.1.1.2 Search for all travel needs specified in the enabling agreement (such as hotels and airports) by US Zip Codes

7.14.1.1.3 View the price of bookings in USD

7.14.1.1.4 Retrieve reports for REDACTED TEXT bookings only, and in USD

7.14.1.1.5 Place air bookings with US and Canadian Domestic carriers, as well as all other airlines as made available by the CCS Air Programme.

7.15 **ACCOUNT MANAGEMENT**

7.15.1. The Supplier shall provide an account management and relationship management service which fully supports all of the requirements of the Commercial Agreement and the needs of the Customer which fully supports all of the requirements as detailed within section 7 of this Statement of Requirements.

7.15.2. The Supplier shall provide the Customer with a named Account Manager and a Deputy in the event the main Account manager is not available, within 5 working days of signing the Enabling Agreement. The nominated Account Manager shall have a minimum of two years business travel industry experience in a similar role and shall work closely with the nominated Commercial Agreement manager to deliver the Service.

7.15.3. The Supplier shall provide an account management structure.

7.15.3.1. The Account Manager shall hold regular meetings with the Customer. Monthly meetings will be held with the Customer contract manager and REDACTED TEXT collectively.

7.15.3.2. The Account Manager shall promote, deliver and communicate transparency of pricing, and savings to the Customer respectively.

7.15.3.3. The Supplier shall support the Customer in providing frequent communications to the Customer's user base about the Supplier's booking abilities. One such requirement is for production of a quarterly Newsletter for distribution to all MOD bookers, highlighting booking behaviours and ways to reduce travel spend and important updates regarding the travel service. Full details of what the newsletter should include will be agreed during implementation stage and the monthly performance meetings.

7.15.3.4. Instead of four FOC training sessions per year, as required in 5.12 of Schedule 2B: Part B, the Supplier shall be required to hold FOC information stalls at locations of the Customer's choosing, within the UK, no less than four (4) times per year.

7.15.3.5. The Supplier shall, in an effort to reduce the Customers travel spend, provide audit programmes with the aim to alter high value bookings to more cost-effective options, when within the agreed criteria. The audit thresholds to target such bookings will be agreed at the Implementation stage, as well as a savings target for the Supplier, and the savings generated from such activity is to be presented at each quarterly review meeting. The method of Audit is to be presented by the Supplier, however such methods could include identifying high value flights that can be altered to a substantially cheaper flight but at a similar time and quality of service, or amending hotel bookings when lower rates have become available on the market, or issuing messaging to prompt travellers that they can alter their ticket for a lower rate, post booking completion. The number of potential transactions that could result in a successful saving opportunity will vary depending on the parameters set up at implementation, however for the purposes of the tender the Supplier should assume a minimum of 5% of all travel bookings will have a successful saving opportunity, and bid accordingly. The Supplier shall submit pricing for this task in Appendix E, however the Supplier will be expected to meet the saving target as mentioned above. The Supplier shall only charge for successful instances of a fare reduction, in line with the criteria set out during implementation.

7.15.4. REDACTED TEXT

7.15.5. The Supplier Account Managers shall be proactive around any changes that may affect service, ie. Brexit.

7.16 **CUSTOMER IMPLEMENTATION**

7.16.1. The Supplier shall outline their proposed project implementation plan to clearly state how they plan to manage the transition of services and provide assurance that the Customer's go live date is met. The proposed plan will form part of the Enabling Agreement.

7.16.2. This plan should include a range of named personnel charged with overseeing specific aspects of the encompassing implementation period, who hold the relevant expertise and knowledge to do so effectively (ie Personnel who have an expert knowledge of Security considerations to oversee this aspect of implementation).

7.16.3. This plan should also contain a comprehensive and realistic time scale, ensuring that all Requirements outlined within both this Enabling Period and Schedule 2

Part B of the Commercial Agreement are in place and ready to 'Go Live' at the time of Contract Commencement.

7.16.4. This plan will also contain a comprehensive and fully mapped Risk Register, highlighting and providing mitigations for any anticipated or potential risks to the contract or services provided as part of it.

7.16.5. This Risk Register will inform a Business Continuity Plan which will also be required which will show how any Suppliers intends to react swiftly and comprehensively in the event that the Service were to go down (at the point of implementation, or at any time within the Contract Period).

7.16.6. The Risk Register shall be reviewed on an annual basis.

7.16.7. The Supplier shall carry out due diligence as part of the bid preparation process to ensure that implementation plans and costs take account of all potential dependencies and risks inclusive of those associated to system/process integration, installation, connectivity or other I.T. activity as required by the Customer.

7.16.8. The Supplier shall ensure that Implementation and Go live requirements as detailed within Schedule 2 Part B apply.

7.16.9. The Supplier will provide the Implementation Plan as part of their bid and will arrange a meeting with key personnel between themselves and the Customer to agree and refine this within 30 working days of Contract Award.

7.17 **CORE WORKING HOURS AND OUT OF HOURS**

7.17.1 The Supplier shall ensure that the following Helpdesk Core Hours are adhered to:

7.17.1.1. For Rail & Air: 07:00 - 22:00 GMT (or BST as appropriate) and for Accommodation: 07:00 - 22:00 GMT (or BST as appropriate) Monday to Friday including UK public holidays

7.17.1.2. The Supplier shall ensure that provision, where applicable, is in place to support Travellers with Out of Hours assistance in booking travel. Out of Hours shall fall outside of the Core Hours as defined in section 7.

8. key milestones

8.1. The Supplier should note the following indicative project timeline that the Customer has the right to change:

Milestone	Description	Timeframe
1	Initial Inception Meeting (to include Implementation Plan discussions) Meeting with Incumbent to discuss Transition The Supplier shall prepare the Mobilisation and Delivery Plan; to include but not be limited to; Impact and Mitigation Analysis Key Milestones and Implementation/Project Plan Engagement and Communications Plan Mobilisation and Delivery Plan agreed	04/03/2019
2	Contract Signed (to include agreed Implementation Plan)	06/03/2019
3	Profile build in Digits; i.e. Online user registrations, Profile content agreed, etc.	To be agreed at Implementation
5	User acceptance Testing; i.e. Group of MoD and Dstl Users identified to test ahead of go-live and feedback for any improvements.	To be agreed at Implementation
6	Training plan agreed Communications plan agreed	To be agreed at Implementation
7	Target Go Live	01/07/2019

9. reporting

9.1. The following requirements detail the reporting that is required under this contract.

9.1.1. The Supplier shall provide the ability for the Customer to locate its personnel around the world on an intuitive interactive world map based on the booking data of its travellers. Restriction of access to this facility is to be discussed during implementation.

9.1.2. The Supplier shall reconcile any spend that does not contain a Unit Identity Number (UIN) and has been charged to the Customer's lodged cards for hotels. The reconciliation objective is to either retrieve a refund from the market, by challenging the charge where an incorrect charge has occurred, or to find the correct booking information and UIN so that the correct business area can be billed. The hotel lodged cards requires up to 900 lines to be reconciled each month. Details of how this service will operate will be agreed during the implementation stage, but it shall be priced for in the Suppliers response in Appendix E. The Supplier shall only charge the Customer when a successful reconciliation or refund has occurred. The Supplier should be aware that this requirement may become obsolete should the Customer choose to implement a new payment system to replace the hotel lodged card.

9.1.3. The Supplier shall provide a Monthly update to the Customer as to the progress of the unmatched UIN's. This update shall contain all details reasonably requested by the Customer and shall be provided to a person nominated by the Customer (as may be updated by the Customer from time to time).

9.1.4. The Supplier shall support the Customer in Fraud investigations and Parliamentary questions by providing any reporting information requested within three (3) Working Days of the request.

9.1.5. The Supplier shall also help with the detection and investigation of any potential or suspected fraudulent activity, notifying the Customer as soon as any fraudulent activity is suspected.

9.1.6. The Supplier shall include lost opportunity reporting.

9.1.7. The Supplier shall provide support with Parliamentary Question's, with varying timescales for response, and Freedom of Information requests (20 working days) within the timescales.

9.1.8. The Supplier shall supply all information for adhoc queries on request, in the agreed format, within five (5) Working Days of request. Adhoc queries are one off requests required to support the business. The Customer typically raises ten such queries per month. Adhoc queries can include but are limited to, UK domestic air over a certain period, travel history for a list of travellers, or number of bookings at requested hotel.

9.1.9. The Supplier shall complete and upload the template for all travel spend to the Customer's Third-Party supplier who are responsible for merging travel data with account spend data, by no later than 3rd of each Month for the duration of the Contract Period. (The template and formatting will be provided by the enabling Customer during the implementation stage, along with the relevant contact information).

9.1.10. The Supplier shall provide the Customer with an online reporting tool, allowing nominated users to produce their own tailored multi-dimensional reports using any and / or all the reporting fields as set out.

9.1.11. The Supplier shall complete and upload (to a secure portal) all supplementary/out of policy/missed saving reports, by no later than the 14th of each month (the template for reports shall be detailed during the implementation stage).

9.1.12. The Supplier shall provide a Performance Report on SLA's and KPIs to support Service credits due to the Customer.

9.1.13. When receiving monthly supplementary reports (which will hold information including, but not limited to, out of policy bookings, or bookings made against non-lodged cards), the Customer requires the information/data to be split out by each Business Area to allow the Customer to disseminate them accordingly. REDACTED TEXT. Access shall be locked down so that only nominated personnel are able to access information pertinent to their own area.

9.1.14. All reporting shall be agreed and finalised post award.

10. Volumes

10.1. The Customer's forecasted booking volumes are available in the ITT Pricing Basket (see Appendix E).

11. Complaints/Issue Management and Dispute resolution

11.1. The Supplier shall adhere to the complaints procedure as per the Commercial Agreement.

11.2. The Supplier is required to adhere to the Dispute Resolution Procedure as defined in the Commercial Agreement, Schedule 14, Paragraph 6.

12. Continuous improvement

12.1. The Supplier is expected to continually improve the way in which the required Services are delivered throughout the Contract duration.

12.2. The Supplier should present new ways of working to the Customer during the Monthly Contract review meetings.

12.3. Changes to the way in which the Services are to be delivered must be brought to the Customer's attention and agreed prior to any changes being implemented.

12.4. The Supplier shall present innovative initiatives to the Customer at each monthly Contract review meeting with the aim to either achieve cost savings, reduce fraud, or improve the customer service for the Customer. Cost savings are to be achieved either through efficient improvements in the Service, by targeting booker behaviour to book by more economical means, or by any other means the supplier wishes to present to the Customer. The savings, or benefits, of these initiatives shall be tracked by the Supplier using methodologies agreed between the Supplier and the Customer during the implementation stage and the results of these initiatives shall be presented at the monthly Contract review meeting.

12.5. If requested to do so the Supplier shall develop a Continuous Service Improvement Plan.

13. Sustainability

13.1. The Supplier shall be responsible for the sustainability of the Services and Supplier's systems and shall at all times provide a level of sustainability which is in accordance with Good Industry Practice, the Law, the Standards, and any sustainability requirements as set out in Schedule 19 – Sustainability and Social Value and elsewhere in the Commercial Agreement.

14. Quality

14.1. The Supplier shall be responsible for the quality of all articles or services obtained through Third Party suppliers that engage with delivery of this Service.

14.2. The Supplier shall provide quality assurance throughout the supply chain, including the operation of all relevant ISO industry standards as specified in Schedule 19 – Sustainability and Social Value and elsewhere in the Commercial Agreement.

14.3. The Supplier shall provide the Customer with a proposed Quality Plan which will be agreed between the two Parties, reviewed and maintained, with agreed updates throughout the duration of the Enabling Agreement.

15. Business continuity requirements and crisis management

15.1. The Supplier shall provide a robust Business Continuity and Crisis Management Plan in place to:

15.1.1. Detail the processes in place to maintain the delivery of Services during periods of unplanned unavailability of the Online Booking System and/or Offline Booking Service, including, but not limited to, communication to Customers, Bookers and Travellers;

15.1.2. Detail the processes by which Travellers will be supported in the event of incidents of significant scale and impact, including but not limited to, how information on Travellers who may be impacted will be made available to the Customer, how you will communicate with the impacted or potentially impacted Travellers, what support you will provide to Travellers and how you will provide it.

15.2. The Supplier shall ensure the Business Continuity and Crisis Management Plan is fit for purpose including, but not limited to, testing, reviewing and updating at least once every twelve-Month period and after any major incident.

15.3. REDACTED TEXT

15.4. The details of the Supplier process for the management of the potential incident shall be clearly defined in the Crisis Management plan.

15.5. REDACTED TEXT

15.5.1. REDACTED TEXT

15.5.2. REDACTED TEXT

16. PRICE

16.1. Prices are to be submitted via the Appendix E excluding VAT.

16.2. The Supplier shall submit Booking fee model fixed prices for the duration of the Agreement with the Customer.

16.3. Prices on the booking portal shall be displayed in Pounds Sterling including VAT, with the exception of BDS-US as stated in paragraph 7.14.

16.4. The Customer reserves the right not to award, any costs incurred are the Suppliers own as per Appendix A Section 10.

17. STAFF AND CUSTOMER SERVICE

17.1. The Customer requires the Supplier to provide a sufficient level of resource throughout the duration of the Provision of Offline and Online Travel Management solutions to the Customer agreement to consistently deliver a quality service to all Parties 24 hours a day, 7 days a week, 365 days a year. (366 days if in a leap year)

17.2. Supplier's staff assigned to the Provision of Offline and Online Travel Management solutions to the Customer agreement shall have the relevant qualifications and experience to deliver the solution.

17.3. The Supplier shall ensure that staff understand the Customer's vision and objectives and will provide excellent customer service to the Customer and/or the Booker/traveller throughout the duration of the Enabling Agreement. This will be discussed as part of the monthly review meetings.

18. Service levels and performance

18.1. The Customer will measure the quality of the Supplier's delivery by enforcing the Service Level Agreements (SLA's) detailed in Annex B of this Appendix B Statement of Requirements.

18.2. For the purpose of the Service Credit calculations each Service Credit is equal to the sum of one pound (£1).

18.3. The Supplier shall adhere to all mechanisms for remedies of poor performance such as service credits in accordance with the processes agreed in the PSTVS Commercial Agreement Schedule 3-Service Levels and Service Credits.

18.4. The Service credit shall apply in respect of any failure by the Supplier to meet one (1) or more Service levels.

18.5. Failure to meet any Service Level for two consecutive months will require a Rectification Plan being produced and shared with the Authority and/or the Customer and implemented after month two (2).

18.6. Failure to meet any target for three (3) months in a row, will require a performance meeting with the Authority and/or the Customer at senior level.

18.7. If a Service Level is not met for two months in a row, the service credit doubles in the second month. If Service Level not met for a third month in a row, service credit triples. For example: 100 credits for failing one month, if failing for a second month 200 service credits will be applied (with a Rectification Plan), if failing for a third month in a row 300

service credits will apply. If this has been identified, the Supplier shall attend a performance review meeting the Customer(s) providing them with a Rectification Plan to the issues identified.

19. Security requirements

REDACTED TEXT

20. Payment

20.1. REDACTED TEXT.

20.2. Invoices are to be presented to the Customer in an agreed format and timescales each month following the last day of each month. The invoice to the Customer must clearly show the Suppliers booking fees incurred for that month. Consolidated invoices are to be presented to MOD DBS Liverpool with sufficient detail captured at the time of booking to enable accurate charging of business areas and cost centres

20.3. The Supplier shall accept and maintain an accurate up to date cost centre and UIN list within their database and only permit bookings against active accounts using current agreed cost centre codes that the online booking tool must validate before a booking is accepted. The process and format of uploads and amending these codes will be agreed at the implementation stage.

20.4. The Customer is currently conducting a review on its payment processes and it may wish to change the payment process during the contract period.

20.5. The Supplier shall support the Customer by implementing any new payment solutions (such as single use virtual cards) during the contract period.

20.6. As per Condition 17.13.1.8 (REDACTED TEXT ONLY REQUIREMENTS), The Supplier shall provide, and manage, a virtual card solution for REDACTED TEXT. Payment will be made via weekly consolidated invoicing as detailed above

21. Location

21.1. The Supplier shall conduct Travel services at their own premises.

21.2. The Customer procurement and contract management team responsible for this requirement will be located at:

MOD Abbey Wood
REDACTED TEXT

ANNEX 2b - Outputs from Direct Award / Further Competition

HRG is contractually committed to the proposal detailed in this Annex unless otherwise explicitly stated elsewhere in this Enabling Agreement, however all statements relating to options are subject to this enabling agreement or contract change and all savings are subject to non-committal targets agreed at implementation, or through continuous improvement.

HRGS Quality responses and Commercial Submission.

REDACTED TEXT

ANNEX 3 – Customer-Level Go Live Implementation Plan

MOD Phase 1 Go Live Date 15th July 2019

MOD Phase 2 Go Live Date – TBC

Dstl Go Live date – 29th July 2019

MOD Phase 2 Go Live to include; MOD Virtual Card solution, Oyster Card availability, Ski Trips.

REDACTED TEXT

ANNEX 4 – Reporting

1. Accurate, timely and comprehensive Management Information (MI) will be required by the Customer to effectively manage the Commercial Agreement.

2. In accordance with Schedule 13 (Management Information), the Supplier shall provide the following MI reports to the Customer:

   2.1. First Class Air (Monthly)

   2.2. First Class Rail (Monthly)

   2.3. First Class Air under 4 hours (Monthly)

   2.4. Hotel Billback (Monthly)

   2.5. Hotel Over Cap Rates (Monthly)

   2.6. Technical Helpdesk call charges (Monthly)

   2.7. Out of hours calls and charges (Monthly)

   2.8. Domestic Count (Monthly)

   2.9. CO2 Emissions (Quarterly)

   2.10 2* and 3* Reports (Quarterly) For this data to be run a list of names will be provided each quarter, by MOD Travel team.

   2.11. POT code 6 and 6v Detached duty reports (Quarterly)

   2.12. Hotel Bookings (Monthly)

3. Accurate, timely and comprehensive Management Information (MI) will be required by the Enabling Authority to effectively manage the Contract. In accordance with Paragraph 7 of Schedule 13 (Management Information), the Supplier shall provide the following MI reports to the Enabling Authority:

   a) Bookings that have been made outside of the Enabling Authority's Travel Policy
   b) Number of accommodation non arrivals (no shows) that has resulted in the accommodation venue applying charges
   c) Changes made throughout the booking lifecycle, enabling Enabling Authorities to identify behavioural trends which occur between booking and travel
   d) "Missed savings", including the value (£s) of missed savings

e) Dashboard summarising the following information, in both a graphical and table format:

f) For all Travel Booking Services:

i. Spend by individual month and cumulative for the reporting year, for each category (i.e. rail, accommodation, air, and booking fees) detailing total spend, number of transactions and average ticket price/room rate in table format, with % spend split in graphical format.
ii. Number and value of refunds and cancellations across air, rail and accommodation.

g) For air:

i. Top 10 suppliers by spend and number of journeys including average fares
ii. Top 10 routes by spend and number of journeys
iii. Top 10 travellers by spend and number of journeys
iv. Number and % of journeys under 300 miles
v. Domestic (UK), short haul and long haul flights, split by spend and volume.

h) For rail:

i. Top 10 routes by spend and number of journeys including average fares
ii. Top 10 travellers by spend and number of journeys
iii. Out of policy bookings detailing number of bookings and spend split by the reason codes defined in Annex 1 of Contract 3 Schedule 2 : Services Part A: Specification of Requirements
iv. % restricted and out of policy tickets for journeys over 50 miles
v. Total value and volume of missed savings opportunities
vi. % spend by ticket type in graphical format
vii. Number and % of bookings by despatch method
viii. Number of first class bookings.

i) For accommodation:

i. Top 10 locations by spend and number of room nights including average room rates
ii. Top 10 accommodation venues by spend and number of room nights
iii. Top 10 accommodation travellers by spend and number of room nights

iv. Out of policy bookings detailing number of bookings and spend split by the reason codes defined in Annex 1 of Contract 3 Schedule 2 : Services Part A: Specification of Requirements

v. Cost incurred where the cost of cancellation or refunds, and fees incurred in administering the cancellation or refunds, outweighs the original transaction cost

4. In addition to the MI reports and information set out above in this Schedule, the Customer and the Supplier agree that the Supplier shall provide the following MI reports and information to the Customer (templates to be provided by the Enabling Authority following award of the Commercial Agreement):

ANNEX 5 – Key Personnel

1. General

1.1. The Supplier has assigned the following Key Personnel to the Enabling Agreement in the Key Roles detailed below:

Key Role	Key Personnel
REDACTED TEXT	***REDACTED TEXT***
REDACTED TEXT	***REDACTED TEXT***
REDACTED TEXT	***REDACTED TEXT***
REDACTED TEXT	***REDACTED TEXT***

ANNEX 6 Transferring Employees

A copy of the TUPE file can be found at **ANNEX A of the ITT,** this is subject to change during the Further Competition. The Final list of Transferring Employees will be listed in this Annex prior to signature of the Enabling Agreement.

No transferring Employees

ANNEX 7 Security Requirements

Official – Sensitive Security Requirements

1. In this condition “Information” means information recorded in any form disclosed or created in connection with the Enabling Agreement.

2. The Supplier shall protect all Information relating to the aspects designated **OFFICIAL-SENSITIVE** (Personal) as identified in the Personal Data Aspects Letter annexed to the Enabling Agreement, in accordance with the official security conditions contained in the Commercial Agreement or the provisions within the Personal Data Aspects Letter.

3. The Supplier shall include the requirements and obligations set out in clause 2 in any sub-contract placed in connection with or for the purposes of the Enabling Agreement which requires disclosure of **OFFICIAL-SENSITIVE** (Personal) Information to the subcontractor or under which any Information relating to aspects designated as **OFFICIAL-SENSITIVE** (Personal) is created by the subcontractor.

4. The Supplier shall also include in the sub-contract a requirement for the subcontractor to flow the requirements of this clause to its subcontractors and through all levels of the supply chain to the lowest level where any **OFFICIAL-SENSITIVE** (Personal) Information is handled.

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

"**Approval Date"**	Has the meaning given in paragraph 5.4.1 of this Security Requirements for Solution 4 (Schedule 5);
“Breach of Security”	the occurrence of: (a) any unauthorised access to or use of the Services, the Customer Premises, the Sites, the “THE SERVICE” Information System and/or any information or data (including the Confidential Information and the Customer Data) used by the Supplier or any Sub-Contractor in connection with this Agreement; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Customer Data), including copies of such information or data, used by the Supplier or any Sub-Contractor in connection with this Agreement; and/or any part of the “THE SERVICE” Information System ceasing to be compliant with the Certification Requirements; in either case as more particularly set out in the Security requirements in Schedule 2: Part B: Specification of Requirements and the Baseline Security Requirements;

"Certification Requirements"	means the requirements given in paragraph 6 of this Security Requirements for Solution 4 (Schedule 5);
"COTS Products"	is software that: (a) the licensor of that software makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the licensor save as to price; and has a Non-trivial Customer Base;
"Information Risk Management Approval"	Is the assessment of any information system by an independent information risk manager/professional which results in a statement that the risks to the information system have been appropriately considered and the residual risks reduced to an acceptable level;
"IT Health Check"	has the meaning given in paragraph 7.1.2 of this Security Requirements for Solution 4 (Schedule 5);
"Risk Management Approval Statement"	Sets out the information risks associated with using the "THE SERVICE" Information System;
"Security Assurance Framework"	has the meaning given in paragraph 7.1.1 of the Security Management (Schedule 5)
"Security Management Plan"	Has the meaning given in paragraph 5.4.1 of this Security Requirements for Solution 4 (Schedule 5);
"Security Tests"	has the meaning given paragraph 7.1.4 of this Security Requirements for Solution 4 (Schedule 5);
""THE SERVICE" Data"	All information (including pensions data) provided to the Supplier by the Customer;
""THE SERVICE" Information System"	Has the meaning given in paragraph 3.1 of this Security Requirements for Solution 4 (Schedule 5);
""THE SERVICE" Statement of Information Risk Appetite"	Has the meaning given in paragraph 4.1 of this Security Requirements for Solution 4 (Schedule 5);
" "THE SERVICE" s Risk Management Documentation"	Has the meaning given in paragraph 5.3 of this Security Requirements for Solution 4 (Schedule 5);
"Vulnerability Correction Plans"	has the meaning given in paragraph 7.2.3 of this Requirements for Solution 4 (Schedule 5);

1 INTRODUCTION

1.1 This Schedule sets out the principles of protective security to be applied by the Supplier in performing its obligations under this Agreement and in delivering the Services.

1.2 This Schedule also sets out:

1.2.1 the process which shall apply to the Information Risk Management Approval of the "THE SERVICE" Information System;

1.2.2 the requirement for the Supplier to ensure that:

(a) each Sub-Contractor who will Process "THE SERVICE" Data; and

(b) any ICT system which the Supplier or its Sub-Contractors will use to store, process or transmit "THE SERVICE" Data,

is and continues to be compliant with the Certification Requirements;

(c) the requirements on the Supplier to conduct Security Tests; and

(d) each Party's obligations in the event of an actual or attempted Breach of Security.

2. Principles of Security

2.1 An IT/Security Working Group shall be established by the Supplier in accordance with Schedule 14 (Governance) to monitor and provide guidance to the Parties during the Information Risk Management Approval of the "THE SERVICE" Information System.

2.2 Each Party shall provide access to members of its information assurance personnel in accordance with the Security Management Plan to facilitate the design, implementation, operation, management and continual improvement of the "THE SERVICE" Risk Management Documentation and the security of the "THE SERVICE" Information System and otherwise at reasonable times on reasonable notice.

3. "THE SERVICE" Information System

3.1 The information assets, ICT systems, associated business processes and/or premises which have been agreed between the parties to constitute the system and

shall be detailed in a diagram included in the “THE SERVICE” Risk Management Documentation.

3.2 The Customer may change the scope of the “THE SERVICE” Information System in accordance with the process set out in Annex 1 of Schedule 18 (Enabling Agreement).

4. Statement of Information Risk Appetite and Baseline Security Requirements

4.1 The Customer has provided the Supplier with its Statement of Information Risk Appetite for the “THE SERVICE” Information System and the Services (the " “THE SERVICE” Statement of Information Risk Appetite").

4.2 The Customer's Baseline Security Requirements in respect of the “THE SERVICE” Information System are set out in Appendix 1.

4.3 The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Information Risk Management Approval of the “THE SERVICE” Information System.

5. Information Risk Management Approval of the “THE SERVICE” Information System

5.1 The “THE SERVICE” Information System shall be subject to Information Risk Management Approval in accordance with this Paragraph 5 and reviewed annually.

5.2 Information Risk Management Approval of the “THE SERVICE” Information System shall be performed by representatives appointed by the Customer.

5.3 The Supplier shall prepare risk management documentation (the" “THE SERVICE” Risk Management Documentatio**n**") for any part of the “THE SERVICE” Information System which is not subject to a separate Risk Management Approval process,

which shall be subject to approval by the Customer in accordance with this Paragraph 5.

5.4 The “THE SERVICE” Risk Management Documentation shall be structured in accordance with the template as agreed with the Customer and include:

5.4.1 an initial Security Management Plan which shall include:

(a) address the security delivery objective described in Appendix 1;

(b) the dates on which each subsequent iteration of the “THE SERVICE” Risk Management Documentation will be delivered to the Customer for review and staged approval;

(c) the date by which the “THE SERVICE” Information System must achieve Risk Management Approval and acceptance of residual risks ("Approval Date"); and

(d) the tasks, milestones, timescales and any dependencies on the Customer or Customers for the approval of the “THE SERVICE” Information System.

5.4.2 a risk assessment, risk register and risk treatment plan for the “THE SERVICE” Information System;

5.4.3 a completed ISO 27001:2013 Statement of Applicability (SoA) for the “THE SERVICE” Information System; and

5.4.4 evidence that the Supplier and each applicable Sub-Contractor is compliant with the Certification Requirements.

5.5 To facilitate Information Risk Management Approval of the “THE SERVICE” Information System, the Supplier shall provide the Customer and its authorised representatives with:

5.5.1 access to the Sites and the information assets within the “THE SERVICE” Information System on request or in accordance with the Information Risk Management Approval Plan; and

5.5.2 such other documentation that they may reasonably require, to enable the Customer to establish that the “THE SERVICE” Information System is compliant with the “THE SERVICE” s Risk Management Documentation.

5.6 The Customer shall, by the relevant date set out in the Information Risk Management Plan, issue a Risk Management Approval Statement which will form part of the “THE SERVICE” s Risk Management Documentation (“THE SERVICE” Risk Management Approval Statement ") confirming either:

5.6.1 that the Customer is satisfied that the identified risks to the “THE SERVICE” Information System have been adequately and appropriately

addressed and that the residual risks are understood and accepted by the Customer.

5.6.2 the Customer considers that the residual risks to the "THE SERVICE" Information System have not been reduced to a level acceptable by the Customer.

5.7 The Supplier acknowledges that it shall not be permitted to use the "THE SERVICE" Information System to receive, store or Process any "THE SERVICE" Data prior to receiving Information Risk Management Approval from the Customer.

5.8 The Supplier shall keep the "THE SERVICE" Information System and "THE SERVICE" Risk Management Documentation under review and shall update this documentation at least annually and whenever, in respect of the

"THE SERVICE" s Information System and/or the "THE SERVICE" Risk Management Documentation, the Supplier becomes aware (including by way of a notification or otherwise), or should reasonably have been or become aware (including by way of a notification or otherwise) that:

5.8.1 there is a significant change to the components or architecture of "THE SERVICE" Information System;

5.8.2 a new risk or vulnerability is identified to the components or architecture of the "THE SERVICE" Information System;

5.8.3 there is a change in the threat profile;

5.8.4 a Sub-Contractor fails to comply with the "THE SERVICE" Information System Certification Requirements;

5.8.5 there is a significant change to any risk component;

5.8.6 there is a proposal to change any of the Sites from which any part of the Services are provided;

5.8.7 an ISO27001 audit report produced in connection with the ISO27001 certification requirements indicates significant concerns;

and the Supplier shall submit each update to the "THE SERVICE" Information Risk Management Documentation to the Customer for approval as appropriate.

5.9 The Supplier shall review each Change Request against the "THE SERVICE" Information Risk Management Documentation to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the "THE SERVICE" Information Risk Management Documentation, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Customer.

5.10 The Supplier shall be solely responsible for the costs associated with developing and updating the "THE SERVICE" Information Risk Management Documentation

and carrying out any remedial action required by the Customer as part of the Information Risk Management Approval process.

6. Certification Requirements

6.1 The Supplier shall ensure that at all times during the Term that:

6.1.1 the Supplier; and

6.1.2 any Sub-Contractor that has access to “THE SERVICE” information,

are Certified as compliant with ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing Certification of compliance with ISO/IEC 27001:2013 and are Certified as compliant with Cyber Essentials and shall provide the Customer with a copy of each such Certificate of compliance before the Supplier shall be permitted to use the “THE SERVICE” Information System to receive, store or Process any Customer Data.

6.2 The Supplier shall ensure that at all times during the Term that each Sub-Contractor who is responsible for the secure destruction of “THE SERVICE” Data, is Certified as compliant with Cyber Essentials and:

(a) Certified as compliant with ISO/IEC 27001:2013;

(b) included within the scope of an existing Certification of compliance with ISO/IEC 27001;

(c) provides that service on Sites which are included within the scope of an existing Certification of compliance with ISO/IEC 27001:2013; or

(d) Certified as compliant with the CESG Assured Service (CAS) Service Requirement Sanitisation Standard.

In respect of each such Sub-Contractor, the Supplier shall provide the Customer with evidence of that Sub-Contractor's compliance with the requirements set out in this paragraph before the Supplier shall be permitted to transfer “THE SERVICE” Data to the relevant Sub-Contractor.

6.3 The Supplier shall notify the Customer as soon as reasonably practicable and, in any event within 2 Working Days, should any Sub-Contractor cease to be compliant with the Certification Requirements and, on request from the Customer procure that the relevant Sub-Contractor:

6.3.1 immediately ceases using the “THE SERVICE” Data; and

6.3.2 procure that the relevant Sub-Contractor promptly returns, destroys and/or erases the “THE SERVICE” Data in accordance with Baseline Security Requirements.

7. Security Testing

7.1 The Supplier shall, at its own cost and expense:

7.1.1 undertake the security assurance activities as defined in the “Authority's” Security Assurance Framework. The Supplier can propose alternative security testing not defined in the Security Assurance Framework but shall need to demonstrate to the satisfaction of the “Authority's” security

assurance lead that the proposed security test delivers comparable level of assurance to test defined in the Security Assurance Framework.

7.1.2 procure a CHECK IT Health Check of the “THE SERVICE” Information System by a CESG approved member of the CHECK Scheme once every 12 months during the Term (each an "IT Health Check") unless additional IT Health Checks are required by Paragraph 7.2;

7.1.3 conduct vulnerability scanning and assessments of the “THE SERVICE” Information System monthly;

7.1.4 conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-Contractors of a critical vulnerability alert from a Supplier of any software or other component of the “THE SERVICE” Information System to determine whether the vulnerability affects the “THE SERVICE” Information System; and

7.1.5 conduct such other tests as are required by:

(a) any Vulnerability Correction Plans;

(b) the ISO27001 certification requirements;

(c) the “THE SERVICE” Information Risk Management Documentation; and

(d) the Customer following a Breach of Security or a significant change to the components or architecture of the “THE SERVICE” Information System,

(each a "Security Test").

7.2 In relation to each IT Health Check, the Supplier shall:

7.2.1 agree with the Customer the aim and scope of the IT Health Check;

7.2.2 promptly, following receipt of each IT Health Check report, provide the Customer with a copy of the IT Health Check report;

7.2.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(a) prepare a remedial plan for approval by the Customer (each a "Vulnerability Correction Plan") which sets out in respect of each vulnerability identified in the IT Health Check report:

(i) how the vulnerability will be remedied;

(ii) the date by which the vulnerability will be remedied;

(iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Customer,

include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) in respect of each vulnerability identified in the IT Health Check report comply with the Vulnerability Correction Plan; and

(c) conduct such further Security Tests on the "THE SERVICE" Information System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

7.3 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Service and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Customer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

7.4 The Customer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Customer with the results of such Security Tests (in a form approved by the Customer in advance) as soon as practicable after completion of each Security Test.

7.5 Without prejudice to any other right of audit or access granted to the Customer pursuant to this Agreement, the Customer and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the "THE SERVICE" Information System and/or the Supplier's compliance with the "THE SERVICE" Information Risk Management Documentation. The Customer shall take reasonable steps to notify the Supplier prior to carrying out such Security Tests to the extent that it is reasonably practicable for it to do so taking into account the nature of the Security Test.

7.6 The Customer shall notify the Supplier of the results of such Security Tests after completion of each such test.

7.7 The Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If such Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance to the extent directly arising as a result of the Customer and/or its authorised representatives carrying out such Security Tests.

7.8 Without prejudice to the provisions of Paragraph 7.2.3, where any Security Test carried out pursuant to this Paragraph 7 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Customer of any changes to the "THE SERVICE" Information System and/or the "THE SERVICE" Information Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Customer's prior written approval, the Supplier shall implement such changes to the "THE SERVICE" Information System and/or the "THE SERVICE" Information Risk Management Documentation and

repeat the relevant Security Tests in accordance with the timetable agreed with the Customer or, otherwise, as soon as reasonably possible.

7.9 If the Customer unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the "THE SERVICE" Information Risk Management Documentation in accordance with paragraph 7.8 above, the Supplier shall not be deemed to be in breach of this Agreement to the extent it can be shown that such breach:

7.9.1 has arisen as a direct result of the Customer unreasonably withholding its approval to the implementation of such proposed changes; and

7.9.2 would have been avoided had the Customer given its approval to the implementation of such proposed changes.

7.10 For the avoidance of doubt, where a change to the "THE SERVICE" Information System and/or the "THE SERVICE" Information Risk Management Documentation is required to remedy non-compliance with the Information Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.

7.11 If any repeat Security Test carried out pursuant to Paragraph 7.8 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.

7.12 On each anniversary of the Commercial Agreement Commencement Date, the Supplier shall provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

7.12.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Agreement; and

7.12.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

8. Breach of Security – General Principles

8.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other within one hour in accordance with the security

incident management process as set out in the "THE SERVICE" Information Risk Management Documentation.

8.2 Without prejudice to the security incident management process set out in the "THE SERVICE" Information Risk Management Documentation, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Customer) necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the "THE SERVICE" Information System against any such potential or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Customer, acting reasonably, may specify by written notice to the Supplier; and

(d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;

8.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Customer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Customer.

8.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance of the "THE SERVICE" Information System and/or the "THE SERVICE" Information Risk Management Documentation with the Baseline Security Requirements and/or this Commercial Agreement, then such action and any required change to the "THE SERVICE" Information System and/or "THE SERVICE" Information Risk Management Documentation shall be at no cost to the Customer.

9. Breach of Security – IT Environment

9.1 The Supplier shall, as an enduring obligation throughout the Term, use its reasonable endeavours to prevent any Breach of Security for any reason including as a result of malicious, accidental or inadvertent behaviour. In accordance with the patching policy (which shall form part of the "THE SERVICE" Information Risk Management Documentation and which shall be agreed with the Customer), this shall include an obligation to use the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.

9.2 Notwithstanding Paragraph 9.1, if a Breach of Security is detected in the Customer System or the "THE SERVICE" Information System, the Parties shall co-operate to reduce the effect of the Breach of Security and, particularly if the Breach of Security causes loss of operational efficiency or loss or corruption of Customer Data, assist

each other to mitigate any losses and to restore the Ordered Services to their desired operating efficiency.

9.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraphs 8 and 9.2 shall be borne by the Parties as follows:

9.3.1 by the Supplier where the Breach of Security originates from defeat of the Supplier's or any Sub-Contractor's security controls, the Supplier Software, the Third Party Software or the "THE SERVICE" Data (whilst the "THE SERVICE" Data was under the control of the Supplier);

9.3.2 by the Customer if the Breach of Security originates from defeat of the Customer's security controls or "THE SERVICE" Data (whilst the "THE SERVICE" Data was under the control of the Customer); and

9.3.3 in all other cases each Party shall bear its own costs.

10. Vulnerabilities and Corrective Action

10.1 The Customer and the Supplier acknowledge that from time to time vulnerabilities in the "THE SERVICE" Information System will be discovered which unless mitigated will present an unacceptable risk to the "THE SERVICE" Data.

10.2 The severity of threat vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the "THE SERVICE" Information Risk Management Documentation and using the appropriate vulnerability scoring systems including:

10.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS as set out by NIST https://nvd.nist.gov/vuln-metrics/cvss); and

10.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

10.3 The Supplier shall procure the application of security patches to vulnerabilities in the "THE SERVICE" Information System within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 7 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

10.3.1 the Supplier can demonstrate that a vulnerability in the "THE SERVICE" Information System is not exploitable within the context of the Services (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of the Services must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Services;

10.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the

Supplier had followed and continues to follow the security patch test plan agreed with the Customer; or

10.3.3 the Customer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the "THE SERVICE" Information Risk Management Documentation.

10.4 The "THE SERVICE" Information Risk Management Documentation shall include provisions for major version upgrades of all Supplier Software and Third Party Software which are COTS Products to be kept up to date such that all Supplier Software and Third Party Software which are COTS Products are always in mainstream support throughout the Term unless otherwise agreed by the Customer in writing.

10.5 The Supplier shall:

10.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

10.5.2 promptly notify GovCertUK of any actual or sustained attempted Breach of Security;

10.5.3 ensure that the "THE SERVICE" Information System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

10.5.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the "THE SERVICE" Information System by actively monitoring the threat landscape during the Commercial Agreement Term;

10.5.5 pro-actively scan the "THE SERVICE" Information System for vulnerable components and address discovered vulnerabilities through the processes described in the "THE SERVICE" Information Risk Management Documentation;

10.5.6 from the date specified in the Information Risk Management Approval plan and within 5 Working Days of the end of each subsequent month during the Term, provide the Customer with a written report which details both patched and outstanding vulnerabilities in the "THE SERVICE" Information System and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

10.5.7 propose interim mitigation measures to vulnerabilities in the "THE SERVICE" Information System known to be exploitable where a security patch is not immediately available;

10.5.8 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the "THE SERVICE" Information System); and

10.5.9 inform the Customer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the

security of the "THE SERVICE" Information System and provide initial indications of possible mitigations.

10.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Supplier shall immediately notify the Customer.

10.7 A failure to comply with Paragraph 10.3 shall constitute a material Default.

11. Data Processing, Storage, Management and Destruction

11.1 The Supplier and Customer recognise the need for the "THE SERVICE" Data to be safeguarded under the UK Data Protection regime. To that end, at all times the Supplier must be able to state to the Customer the physical locations within the UK where the "THE SERVICE" Data may be stored, processed and managed.

11.2 Where part or all of the Services are not delivered from within the UK;

The Supplier shall obtain approval from the Authority's Data Controller/Information Risk Owner through the Authority for the off-shored elements. However, if the Supplier needs to exchange the Authority or Customers' information with an off shored third party service provider on an individual travel transactional basis (i.e. with a Hotel) then there is NO requirement to obtain the Authority's approval for this aspect of the service.

The Supplier will process the Customer's Personal Identifiable Information (PII) and privacy related data in compliance with current UK legislation and in particular the Data Protection Act or other applicable HMG Security Policy. Prior to completion of the Customer Enabling Agreement the Supplier shall be required to support the Customer in obtaining the relevant Customer Data Controller's approval. In support of this approval the Supplier shall be required to produce, to be agreed by the Customer before the Commencement Date of the Customer Enabling Agreement, a Privacy Impact Assessment (PIA).

11.3 The Supplier shall:

11.3.1 on demand, provide: the Customer with all "THE SERVICE" Data in an agreed open format;

11.3.2 have documented processes to guarantee availability of "THE SERVICE" Data in the event of the Supplier ceasing to trade;

11.3.3 securely erase any or all "THE SERVICE" Data held by the Supplier when requested to do so by the Customer; and

11.3.4 securely destroy all media that has held "THE SERVICE" Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, in accordance with Good Industry Practice.

12 Audit and Monitoring

12.1. The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

i. Logs to facilitate the identification of the specific asset which makes every outbound request external to the "THE SERVICE" Information System. To the extent the design of the "THE SERVICE" Information System and Services allows such logs shall include those from DHCP

servers, HTTP/HTTPS proxy servers, firewalls and routers;

ii. Regular reports and alerts setting out details of access by users of the "THE SERVICE" Information System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of "THE SERVICE" Data; and

iii. Security events generated in the "THE SERVICE" Information System and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktop and server operating systems and security alerts from third party security software.

12.2 The Supplier and the Customer shall work together to establish any additional audit and monitoring requirements for the "THE SERVICE" Information System.

12.3 The Supplier shall retain audit records collected in compliance with this Paragraph 12 for a period of at least 6 months.