DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	C285690
THE BUYER:	**NHS England**
BUYER ADDRESS	**7-8 Wellington Place, Leeds, LS1 4AP**
THE SUPPLIER:	KPMG LLP
SUPPLIER ADDRESS:	15 Canada Square, London, E14 5GL
REGISTRATION NUMBER:	OC301540
[redacted]:	[redacted]

DPS SUPPLIER REGISTRATION SERVICE ID: SQ-P3JH3TE

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 10th May 2024.
It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
Non-assured NCSC Services, Risk Assessment, Security Architecture, Security Specialist, Security Strategy, Cyber Transformation, Policy Development, Cyber Essentials Plus, Clearance: Security Check, ISO 27001

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

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM3764iii
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)

- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

- Order Schedules for RM3764iii
  - Order Schedule 1 (Transparency Reports)
  - Order Schedule 4 (Order Tender)
  - Order Schedule 5 (Pricing Details)
  - Order Schedule 6 (ICT Services)
  - Order Schedule 7 (Key Supplier Staff)
  - Order Schedule 8 (Business Continuity and Disaster Recovery)
  - Order Schedule 9 (Security) Part B
  - Order Schedule 15 (Order Contract Management)
  - Order Schedule 20 (Order Specification)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6
7. Order Schedule 4 (Order Tender) as long as any parts of the Order Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

ORDER SPECIAL TERMS
The following Special Terms are incorporated into this Order Contract:

The Core Terms shall be amended with deletions scored-through and insertions underlined as follows:

Special Term 1: Clause 3 (What needs to be delivered)

The following wording shall be included as **new Clauses 3.4, 3.5 and 3.6** of the Core Terms, and references to these clauses shall also be added to clause 10.5.7:

"3.4 The Supplier warrants that it shall comply throughout the term, and following any termination or expiry of the Contract shall continue to comply, with the data security and protection toolkit (DSP Toolkit), an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards and supports key requirements of the GDPR, which can be accessed from https://www.dsptoolkit.nhs.uk/, as may be amended or replaced by the Buyer or the Department of Health and Social Care from time to time.

3.5 The Supplier further warrants and represents that it shall comply throughout the term, and following any termination or expiry of the Contract shall continue to comply, with:

(a) the Baseline Security Requirements (as set out in Appendix 1 of Order Schedule 9 (Security) Part B;

(b) Good Industry Practice;

(c) the Buyer's Security Policy and the ICT Policy;

(d) HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

(e) ISO/IEC27001 and ISO/IEC27002.

3.6 The Supplier warrants and represents that for any system which holds any protectively marked Government Data it shall comply throughout the term, and following any termination or expiry of the Contract shall continue to comply with:

(a) the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications

(b) guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets

(c) the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection

(d) government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

(e) the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles".

Special Term 2: Clause 9.1 Intellectual Property Rights (IPRs)

An additional bullet shall be added to **Clause 9.1 (Intellectual Property Rights), and clause 9.2 shall be varied** as follows:

"9.1. Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to:

- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier

- develop and provide products and services to third parties."

9.2 Any New IPR created under an Order Contract is owned by the Buyer. The Buyer gives the Supplier i) a licence to use any Buyer Existing IPRs and New IPR during the Order Contract Period for the purpose of fulfilling its obligations under the Order Contract. The Supplier may at any time request a licence to use the New IPRs (excluding any Information which is the Buyers Confidential information or which is subject to the Data Protection Legislation) after the Order Contract period on such terms as the Buyer may set, such request will not unreasonably be withheld. The Supplier acknowledges that where any such request relates to New IPR associated with data, that the Buyer may be restricted by reasons of applicable Law and contract. Nothing in this Contract shall be interpreted as the provision of permission by the Buyer to use Government Data or any New IPR derived from Government Data to develop or train AI or machine learning systems."

Special Term 3: Clause 10.3 (Ending the Contract without a reason)

Clause 10.3.2 shall be amended, and a new Clause 10.3.3 shall be inserted, as follows:

"10.3.2 Each Buyer has the right to terminate their Order Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice and if it's terminated Clause 10.5.2 to 10.5.7 applies. Without prejudice to Clause 10.3.3, the Buyer shall have no liability in respect of any costs incurred by the Supplier arising from such termination.

10.3.3 The Parties acknowledge and agree that:

(a) the Buyer's right to terminate under Clause 10.3.2 is reasonable in view of the subject matter of the Order Contract and the nature of the Deliverables being provided.

(b) the Order Contract Charges paid during the notice period given by the Buyer in accordance with Clause 10.3.2 are a reasonable form of compensation and are deemed to fully cover any avoidable costs or losses incurred by the Supplier which may arise (directly or indirectly) as a result of the Buyer exercising the right to terminate under Clause 10.3.2."

Special Term 4: Clause 14 (Data Protection)

The following wording shall be included as a new **Clause 14.12 (Data Protection)** of the Core Terms:

"14.12. Without limitation to the obligations as set out in Joint Schedule 11 (Processing Data) and the Order Form, the Supplier shall:

14.12.1 provide a draft template Data Protection Impact Assessment for the Buyer's review;

14.12.2 consider the Buyer's feedback and shall update the draft template Data Protection Impact Assessment and associated guidance notes, prior to the Start Date of the Contract;

14.12.3 provide a further draft Data Protection Impact Assessment as a part of the Order Procedure for each Deliverable for each commission under the Contract;

14.12.4 be responsible for updating its Data Protection Impact Assessment at each material change of the Deliverables (including but not limited to each release of new software) and following any Variation."

Special Term 5: Clause 23 (Transferring responsibilities)

New clauses 23.7, 23.8 and 23.9 shall be inserted into the Core Terms, as follows:

"23.7 The Supplier may only Sub-Contract all or part of the Deliverables under the Contract with the prior written approval of the Buyer.

23.8 If the Supplier chooses to use Subcontractors, this will be detailed in any bid along with the percentage of delivery allocated to each Subcontractor.

"23.9 Notwithstanding any approval provided by the Buyer pursuant to Clause 23.7, the Supplier remains solely responsible for the provision of the Deliverables in accordance with the terms of the Contract."

Special Term 6 – Clause 19 (The Rights of Third Parties)

Clause 19 (Other people's rights in a contract) of the Core Terms shall be deleted and replaced with the following:

19.1 Subject to Clause 19.2, no third parties may use the Contracts (Rights of Third Parties) Act (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

19.2 Where the Buyer either procures the Deliverables on behalf of, or to be provided to, a third party (such third party being a **Relevant Organisation** for the purposes of this Order Contract), the following shall apply:

19.2.1 the Relevant Organisation(s) may enforce the rights and obligations under this Order Contract; and/or

19.2.2 (without double counting) any Loss suffered or incurred by a Relevant Organisation due to a breach of the Supplier's obligations under this Order Contract shall be deemed to be a Loss of the Buyer, and the Buyer shall be able to recover the same under and in accordance with the terms of this Order Contract.

[redacted]

Special Term 6: DPS Joint Schedule 6 (Key Subcontractors)

The following wording shall be included as a new **Paragraph 1.4.6** of DPS Joint Schedule 6 (Key Subcontractors):

"*1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:*

[redacted]

Special Term 7: DPS Order Schedule 9 (Security)

The following wording shall be included as a new **Part C** of DPS Order Schedule 9 (Security):

Part C: Commodity Service Security Requirements

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

"ISMS" means the information security management system and process developed by the Supplier in accordance with paragraph 2 (ISMS) as updated from time to time; and

"**Security Management Plan**" means the Supplier's security management plan prepared pursuant to paragraph 2.

1. The Supplier will ensure that any Supplier system which holds any protectively marked Government Data will comply with the principles in the Security Policy Framework at:

   - https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
   - guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
   - the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection
   - government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

2. If requested to do so by the Buyer, before entering into this Contract the Supplier will, within 15 Working Days of the date of this Contract, develop (and obtain the Buyer's Approval of) a Security Management Plan and an Information Security Management System. After Buyer Approval the Security Management Plan and Information Security Management System will apply during the Term of this Contract. The/Both plans will protect all aspects and processes associated with the delivery of the Services.

3. The Supplier will immediately notify the Buyer of any breach of security of the Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer Confidential Information however it may be recorded.

4. Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[redacted]

ORDER START DATE: 24th May 2024

ORDER EXPIRY DATE: 23rd May 2027

ORDER INITIAL PERIOD: 3 Years

ORDER OPTIONAL EXTENSION 24 Months

DELIVERABLES
See details in Order Schedule 20 (Order Specification)
To be agreed at individual SOW/project level, however the future Services and Deliverables will be aligned to Order Schedule 20 (Order Specification). The Parties acknowledge that these requirements are not fully defined at the point of awarding this Order Form and will be developed over the Contract Period as several projects ("Future Services"). Future Services will be called off using the Commissioning Process outlined at Appendix 1 to this Order Form.

The Buyer is not obliged to request any Future Services. In the event that the Buyer does raise a request for Future Services, the Supplier is required to respond in accordance with the Commissioning Process outlined in Appendix 1 to this Order Form.

"SOW" means the detailed plan, agreed in accordance with Appendix 1 of this Order Form, describing the Services and/ or Deliverables to be provided by the Supplier, the timetable for their performance and the related matters listed in the template SOW set out in Appendix 2 of the Order Form.

LOCATION
The base location of where the Services will be carried out remotely or at a UK based location. This will be confirmed during the Commissioning Process for each requirement.

MAXIMUM LIABILITY
The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The total capped value of this Order Contract is £4,946,600.

[redacted]

ORDER CHARGES
See details in Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract and in accordance with NHSE Expense Policy

[redacted]

PAYMENT METHOD
Monthly in arrears as per each SOW

BUYER'S INVOICE ADDRESS:
Invoices should be submitted via electronic invoicing Tradeshift.
https://nhssbs.support.tradeshift.com or in the limited circumstances where electronic invoicing is not possible, please email invoices and credit notes to the following email address sbs.apinvoicing@nhs.net with the billing address on the invoice being:
NHS ENGLAND
X24 PAYABLES K005
PO BOX 312
LEEDS LS11 1HP

BUYER'S AUTHORISED REPRESENTATIVE
[redacted]

BUYER'S ENVIRONMENTAL POLICY
NHS England Social Value Charter available online at: https://digital.nhs.uk/about-nhs-digital/technology-suppliers/nhs-digital-social-value-charter

BUYER'S SECURITY POLICY
Appended at Order Schedule 9

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

SUPPLIER'S CONTRACT MANAGER
[redacted]

PROGRESS REPORT FREQUENCY
Monthly/Quarterly

PROGRESS MEETING FREQUENCY
Quarterly review meetings

KEY STAFF

[redacted]

KEY SUBCONTRACTOR(S)

[redacted]

COMMERCIALLY SENSITIVE INFORMATION

Refer to DPS Joint Schedule 4 Supplier's Commercially Sensitive Information

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Tender)

DATA PROTECTION

Data Protection Impact Assessment ("DPIA") Delivery and Assistance

Without limitation to the obligations as set out in Joint Schedule 11 (Processing Data), where expressly agreed in the individual SOW (s), the Supplier shall, at its own cost, participate and provide full co-operation for the completion of any DPIA conducted by the Buyer relating to the Services and any related Deliverables, such participation and co-operation shall include updating the DPIA following each material change of the Services and Deliverables and following any Variation agreed in writing between the Parties.

Status of the Controller

The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under

each Work Order, which will be agreed via the Commissioning Process. This will dictate the status of each Party under the DPA 2018. A Party may act as:

(a) “Controller” in respect of the other Party who is “Processor”;
(b) “Processor” in respect of the other Party who is “Controller”;
(c) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

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

Protection of Personal Data

As of the Order Start Date, it is accepted there is no Processing of Personal Data involved under this Order Contract and that the data table within Joint Schedule 11 (Processing Data) is not final. There is an expectation that both Parties will assess the data processing arrangement when the subsequent requirements and the Commissioning Process are finalised. It is agreed that each Party shall be responsible for ensuring compliance with the Data Protection Legislation, in relation to its Processing of any Personal Data under this Order Contract. Should the Data Processing position change, the Parties acknowledge that the only Personal Data which may be shared under this Order Contract will be set out in the data processing table in each individual Work Order (where applicable), in the form provided at Appendix 2, below. Further, Joint Schedule 11 (Processing Data) must also be complied with by the Parties as a term of this Order Contract.

The Supplier shall comply with any further written instructions with respect to Processing by the Buyer. Any such further instructions shall be incorporated into the data table below.

The details of any Personal Data which may be shared under this Order Contract will be set out in a table in the Work Order in the form of Annex 1 below.

Annex 1 (*Processing of Personal Data*):

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

Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:

	• ***Insert*** *the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer* **The Supplier is Controller and the Buyer is Processor** *The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:* • ***Insert*** *the scope of Personal Data which the purposes and means of the Processing by the Buyer is determined by the Supplier* **The Parties are Joint Controllers** *The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:* • ***Insert*** *the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together* **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:* • *Business contact details of Supplier Personnel for which the Supplier is the Controller,* • *Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller,* • ***Insert*** *the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer*

	Guidance *where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified*
Duration of the Processing	*Clearly set out the duration of the Processing including dates*
Nature and purposes of the Processing	*Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc*
Type of Personal Data	*Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc*
Categories of Data Subject	*Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*Describe how long the data will be retained for, how it be returned or destroyed*

Goods and/or Services

1 The following requirements shall take priority above all terms, conditions and specifications set out in this Order Contract (including without limitation any embedded documents and terms), and the Supplier shall ensure that the software licences meet and conform with the following requirements:

1.1 The Buyer shall be entitled, free of charge, to sub licence the software to any contractor and/or sub-contractor of the Buyer who is working towards and/or is providing services to the Buyer.

1.2 The Buyer's role as national information and technology partner to the NHS and social care bodies involves the Buyer buying services for or on behalf of the NHS and social care entities. Nothing in the licences for any of the software shall have the effect of restricting the Buyer from discharging its role as the national information and technology partner for the health and care system, which includes the ability of the Buyer to offer software and services to the NHS and social care entities. Specifically, any software licensing clause prohibiting 'white labelling', 'provision of outsourcing services' or similar, shall not be interpreted as prohibiting the Buyer's services.

1.3 The Buyer shall be entitled to deploy the software at any location from which the Buyer and/or any contractor and/or sub-contractor of the Buyer is undertaking services pursuant to which the software is being licenced.

1.4 Any software licenced to the Buyer on a named users basis shall permit the transfer from one user to another user, free of charge provided that the Supplier is notified of the same (including without limitation to a named user who is a contractor and/or Subcontractor of the Buyer).

1.5 The Supplier shall ensure that the Buyer shall be entitled to assign or novate all or any of the software licences free of charge to any other central government entity, by giving the licensor prior written notice.

1.6 The Supplier shall notify the Buyer in advance if any software or service permits the Supplier or any third party remote access to the software or systems of the Buyer.

1.7 Where the Supplier is responsible for the calculation of the appropriate number of users for software, and it is later shown there is a shortfall of licences, the Supplier shall be responsible for all costs of the Buyer.

[redacted]

FORMATION OF CONTRACT

BY SIGNING AND RETURNING THIS ORDER FORM (which may be done by electronic means) the Supplier agrees to enter an Order Contract with the Buyer to provide the Services in accordance with the DPS Core Terms.

The Parties hereby acknowledge and agree that they have read the Order Form and the DPS Core Terms and by signing below agree to be bound by this Order Contract.

For and on behalf of the Supplier:

[redacted]

For and on behalf of the Buyer:

[redacted]

Appendix 1: Future Services – Commissioning Process

Commissioning Process - Project specific statement of requirements for future call offs

7.1 Where the Buyer wishes to commission work under this Call Off Contract, it shall:

7.2 Detail the requirements for each individual project including milestones and acceptance criteria ("Project Requirements") substantially in the format set out in the Order Form.

7.3 The Buyer's commercial team will communicate Project Requirements to the Provider whereupon the Provider shall have five (5) working days (or an alternative period as set out by the Buyer upon communicating the Project Requirements) to respond. All commissioning requests shall be routed through the Commercial department/dedicated Commercial Leads

7.4 The Provider shall respond to the Project Requirements (the "Provider's Solution") in the format specified by the Buyer at the point of communicating the project requirements.

7.5 The Provider's Solution shall include details of how the work will be undertaken, a timeline/activity plan along with CV's (if requested) and a summary of the expertise in the proposed resourcing model, it shall also include a detailed price for the delivery of the Project Requirements in the format provided by the Buyer. Where no format is specified, the method used to calculate the price shall be set out in sufficient detail for the Buyer to understand how the price was determined and, as a minimum, the Provider 's pricing will be broken down by the day rates of resources operating on each project and will be no more expensive than the day rates set out in its Tender.

7.6 In most instances, fixed fee or output-based pricing will be used. In other instances, capped T&M will be utilised based on the submitted rate card. The final decision would lie with the Buyer. Within five (5) working days of receipt of the Provider 's Solution, or in any other period the Buyer deems appropriate, it shall review and feedback comments on the Provider 's Solution. Within two (2) working days of the Buyer providing this feedback (or an alternative period as set out by the Buyer upon communicating its feedback) the Provider shall provide a final Provider 's Solution to the Buyer.

7.7 Where the Buyer agrees with the Provider's Solution the Buyer shall sign and return the Provider 's Solution to the Provider for countersigning whereupon the Provider shall commence delivery of the Services detailed in the Project Requirements and Provider 's Solution at the time agreed in the Project Requirements via the Buyer's online portal

7.8 Amendments to Project Requirements (and associated pricing) after the execution of the associated Project Requirements shall follow the Variation process set out in Joint Schedule 2 of the Call-Off Contract and actioned through the Commercial Team

7.9 Close off from projects after the execution of a SOW shall be confirmed and signed off with the programme.

7.10 At any point during or before the Commissioning Process, the Buyer may seek alternative means of delivering the requirement including potentially recompeting the requirement.

7.11 The Call-Off Contract is non-exclusive, and the Buyer does not commit to awarding any work as part of this Call-Off Contract.

Appendix 2 (Template Statement of Work)

Statement of Works (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.

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

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

Date of SOW:	
SOW Title:	
SOW Reference:	
Call-Off Contract Reference:	
Buyer:	NHS England
Supplier:	
SOW Start Date:	
SOW End Date:	
Duration of SOW:	
Key Personnel (Buyer):	
Key Personnel (Supplier):	
Are Subcontractors being used as part of the Delivery?	Yes/No *Yes, state who is being used and their role in the Delivery of this SOW*
Will personal data be shared in the completion of this SOW?	Yes/No *Yes, where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this SOW, the Parties shall complete and comply with the revised Annex 1 attached to this SOW.* *No, no further action is required.*

1 **Call-Off Contract Specification – Deliverables Context**

SOW Deliverables Background:	**Insert** details of which elements of the Deliverables this SOW will address
Delivery phase(s):	**Insert** item and nature of Delivery phase(s)
Overview of Requirement:	**Insert** details

2 **Buyer Requirements – SOW Deliverables**

Outcome Description:

Milestone Ref	Milestone Description	Acceptance Criteria	Due Date
MS01			
MS02			

Security Applicable to SOW:	The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with the Buyer's Security Policies as set out in Schedule 6 (Order Form Template and Order Schedules). If different security requirements than those set out in Schedule 6 (Order Form Template and Order Schedules) apply under this SOW, these shall be detailed below and apply only to this SOW: **Insert if necessary**
Cyber Essentials Scheme:	The Buyer requires the Supplier to have and maintain a **Cyber Essentials Plus Certificate** for the work undertaken under this SOW.
SOW Standards:	**Insert** any specific Standards applicable to this SOW, if none N/A
Additional Requirements:	

Performance Management:

KPIs	KPI Description	Target	Measured by

3 **Supplier Delivery and Resource Plan**

Delivery Plan:
Dependencies on Buyer:

Resource Plan:

Role Ref.	Role Title	Name	No. of Days	Rate	Fee	Employment / Engagement Route (inc. inside/outside IR35)
Total						

N.B. The resources should in the table above will be provided by the Supplier for the duration of the project. If for any reason it is necessary to change the composition of the team, the Supplier will advise the Buyer as soon as possible and endeavour to offer a replacement member with suitable skills and experience.

IR35 Status Determination Statement	
Required	
Not Required.	

Data Protection:

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

SOW Reporting Requirements:

Further to the Supplier providing the management information detailed in Order Schedule 15 (Order Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:

Ref.	**Type of Information**	**Which Deliverable does this requirement apply to?**	**Required regularity of Submission**
1.	insert	insert	insert
2.	insert	insert	insert

Charges

Call Off Contract Charges:	
The applicable charging method(s) for this SOW is:	
1) Capped time and materials (CTM)	
2) Fixed price	
3) A combination of the above charging methods	(specify below)
please detail if specified 3	
The estimated maximum value of this SOW (irrespective of the selected charging method) is:	£**Insert** value
Rate Cards Applicable:	Order Schedule 5 (Pricing Details).

Reimbursable Expenses:	Expenses are recoverable, by agreement, as stated in Schedule 6 (Order Form Template and Order Schedules) in line with NHS E Policy for outcome-based supply contracts.
Reimbursable Expenses are capped at:	Generally none, in which case state 'Not Applicable', however when agreed by NHSE state a monetary cap.

Signatures and Approvals

Agreement of this SOW

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

For and on behalf of the Supplier

[redacted]

For and on behalf of the Buyer

1. Joint Schedule 1 (Definitions)

1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.

1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In each Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings**" as references to obligations under the Contract;

1.3.8 references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract; and

1.3.12 where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

"Accreditations and Standards"	the Accreditations and Standards Filter Category detailed in DPS Schedule 1.
"Additional Insurances"	insurance requirements relating to an Order Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
"Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees;
"Affected Party"	the party seeking to claim relief in respect of a Force Majeure Event;
"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
"Annex"	extra information which supports a Schedule;
"Approval"	the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly;
"Audit"	the Relevant Authority's right to: a) verify the accuracy of the Charges and any other amounts payable by a Buyer under an Order Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) verify the Open Book Data; d) verify the Supplier's and each Subcontractor's compliance with the applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;

	f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; k) verify the accuracy and completeness of any Management Information delivered or required by the DPS Contract;
"Auditor"	a) the Relevant Authority's internal and external auditors; b) the Relevant Authority's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office; e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and f) successors or assigns of any of the above;
"Authority"	CCS and each Buyer;
"Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer"	the relevant public sector purchaser identified as such in the Order Form;

"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Order Contract initially identified in the Order Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
"Buyer Property"	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Order Contract;
"CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
"CCS Authorised Representative"	the representative appointed by CCS from time to time in relation to the DPS Contract initially identified in the DPS Appointment Form and subsequently on the Platform;
"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Order Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Order Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;

"Commercially Sensitive Information"	the Confidential Information listed in the DPS Appointment Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Confidential Information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
"Contract"	either the DPS Contract or the Order Contract, as the context requires;
"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"Contract Period"	the term of either a DPS Contract or Order Contract from the earlier of the: a) applicable Start Date; or b) the Effective Date until the applicable End Date;
"Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
"Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly;
"Controller"	has the meaning given to it in the GDPR;
"Core Terms"	CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under DPS Contracts and Order Contracts;

"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Man Day, of engaging the Supplier Staff, including: i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer; b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets; c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but excluding: a) Overhead; b) financing or similar costs; c) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Order Contract Period whether in relation to Supplier Assets or otherwise; d) taxation; e) fines and penalties;

	f) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Cyber Security Services"	those Service available under this DPS Contract as documented at DPS Schedule 1
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under an Order Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Levy"	has the meaning given to it in Paragraph 8.1.1 of DPS Schedule 5 (Management Levy and Information);

"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of an Order Contract as confirmed and accepted by the Buyer by confirmation in writing to the Supplier. "**Deliver**" and "**Delivered**" shall be construed accordingly;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable) for the period specified in the Order Form (for the purposes of this definition the **"Disaster Period**");
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
"Dispute"	any claim, dispute or difference arises out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as: a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables; b) is required by the Supplier in order to provide the Deliverables; and/or c) has been or shall be generated for the purpose of providing the Deliverables;
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained

	in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"DPA 2018"	the Data Protection Act 2018;
"DPS"	the dynamic purchasing system operated by CCS in accordance with Regulation 34 that this DPS Contract governs access to;
"DPS Application"	the application submitted by the Supplier to CCS and annexed to or referred to in DPS Schedule 2 (DPS Application);
"DPS Appointment Form"	the document outlining the DPS Incorporated Terms and crucial information required for the DPS Contract, to be executed by the Supplier and CCS and subsequently held on the Platform;
"DPS Contract"	the dynamic purchasing system access agreement established between CCS and the Supplier in accordance with Regulation 34 by the DPS Appointment Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;
"DPS Contract Period"	the period from the DPS Start Date until the End Date or earlier termination of the DPS Contract;
"DPS Expiry Date"	the date of the end of the DPS Contract as stated in the DPS Appointment Form;
"DPS Incorporated Terms"	the contractual terms applicable to the DPS Contract specified in the DPS Appointment Form;
"DPS Initial Period"	the initial term of the DPS Contract as specified in the DPS Appointment Form;
"DPS Optional Extension Period"	such period or periods beyond which the DPS Initial Period may be extended up to a maximum of the number of years in total specified in the DPS Appointment Form;
"DPS Pricing"	the maximum price(s) applicable to the provision of the Deliverables set out in DPS Schedule 3 (DPS Pricing);
"DPS Registration"	the registration process a Supplier undertakes when submitting its details onto the Platform;
"DPS SQ Submission"	the Supplier's selection questionnaire response;
"DPS Special Terms"	any additional terms and conditions specified in the DPS Appointment Form incorporated into the DPS Contract;
"DPS Start Date"	the date of start of the DPS Contract as stated in the DPS Appointment Form;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
"Effective Date"	the date on which the final Party has signed the Contract;

"EIR"	the Environmental Information Regulations 2004;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
"End Date"	the earlier of: a) the Expiry Date (as extended by any Extension Period exercised by the Authority under Clause 10.2); or b) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
"Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
"Estimated Year 1 Contract Charges"	the anticipated total charges payable by the Supplier in the first Contract Year specified in the Order Form;
"Estimated Yearly Charges"	means for the purposes of calculating each Party's annual liability under clause 11.2 : i) in the first Contract Year, the Estimated Year 1 Contract Charges; or ii) in any subsequent Contract Years, the Charges paid or payable in the previous Contract Year; or iii) after the end of the Contract, the Charges paid or payable in the last Contract Year during the Contract Period;
"Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
"Expiry Date"	the DPS Expiry Date or the Order Expiry Date (as the context dictates);
"Extension Period"	the DPS Optional Extension Period or the Order Optional Extension Period as the context dictates;
"Filter Categories"	the number of categories specified in DPS Schedule 1 (Specification), if applicable;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance

	and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from: a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract; b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; c) acts of a Crown Body, local government or regulatory bodies; d) fire, flood or any disaster; or e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds;
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);
"General Anti-Abuse Rule"	a) the legislation in Part 5 of the Finance Act 2013; and b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions;
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	goods made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;

"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which: i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract; or b) any Personal Data for which the Authority is the Data Controller;
"Government Procurement Card"	the Government's preferred method of purchasing and payment for low value goods or services; https://www.gov.uk/government/publications/government-procurement-card--2;
"Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HMRC"	Her Majesty's Revenue and Customs;
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including: a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the DPS Pricing/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and

	e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	the plan for provision of the Deliverables set out in Order Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Indemnifier"	a Party from whom an indemnity is sought under this Contract;
"Independent Control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of processing but does so separately from the Controller providing it with Personal Data and "**Independent Controller**" shall be construed accordingly;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Initial Period"	the initial term of a Contract specified on the Platform or the Order Form, as the context requires;
"Insolvency Event"	a) in respect of a person: b) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or c) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or d) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or f) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or h) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

	i) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or j) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;
"Intellectual Property Rights" or "IPR"	a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information; b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and c) all other rights having equivalent or similar effect in any country or jurisdiction;
"Invoicing Address"	the address to which the Supplier shall Invoice the Buyer as specified in the Order Form;
"IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies;
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of processing;
"Key Personnel"	the individuals (if any) identified as such in the Order Form;
"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	any Subcontractor: a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the

	aggregate Charges forecast to be payable under the Order Contract, and the Supplier shall list all such Key Subcontractors on the Platform and in the Key Subcontractor Section in the Order Form;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Man Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks;
"Management Information"	the management information specified in DPS Schedule 5 (Management Levy and Information);
"Management Levy"	the sum specified on the Platform payable by the Supplier to CCS in accordance with DPS Schedule 5 (Management Levy and Information);
"Marketing Contact"	shall be the person identified in the DPS Appointment Form;
"MI Default"	means when two (2) MI Reports are not provided in any rolling six (6) month period;
"MI Failure"	means when an MI report: a) contains any material errors or material omissions or a missing mandatory field; or

	b) is submitted using an incorrect MI reporting Template; or c) is not submitted by the reporting date (including where a declaration of no business should have been filed);
"MI Report"	means a report containing Management Information submitted to the Authority in accordance with DPS Schedule 5 (Management Levy and Information);
"MI Reporting Template"	means the form of report set out in the Annex to DPS Schedule 5 (Management Levy and Information) setting out the information the Supplier is required to supply to the Authority;
"Milestone"	an event or task described as such in the Implementation Plan;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be achieved;
"Month"	a calendar month and "**Monthly**" shall be interpreted accordingly;
"National Insurance"	contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"New IPR"	a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; but shall not include the Supplier's Existing IPR;
"Occasion of Tax Non – Compliance"	where: a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of: i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;

"Open Book Data"	complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Order Contract, including details and all assumptions relating to: a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables; b) operating expenditure relating to the provision of the Deliverables including an analysis showing: i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; ii) manpower resources broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each manpower grade; iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the DPS Contract Period and on an annual basis; f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and h) the actual Costs profile for each Service Period;
"Open Government Licence"	means the licensing terms for use of government intellectual property at: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/
"Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
"Order Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the DPS Contract), which consists of the terms set out and referred to in the Order Form;

"Order Contract Period"	the Contract Period in respect of the Order Contract;
"Order Expiry Date"	the date of the end of an Order Contract as stated in the Order Form;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create an Order Contract;
"Order Form Template"	the template in DPS Schedule 6 (Order Form Template and Order Schedules);
"Order Incorporated Terms"	the contractual terms applicable to the Order Contract specified under the relevant heading in the Order Form;
"Order Initial Period"	the Initial Period of an Order Contract specified in the Order Form;
"Order Optional Extension Period"	such period or periods beyond which the Order Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form;
"Order Procedure"	the process for awarding an Order Contract pursuant to Clause 2 (How the contract works) and DPS Schedule 7 (Order Procedure);
"Order Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Order Contract;
"Order Start Date"	the date of start of an Order Contract as stated in the Order Form;
"Order Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following an Order Procedure and set out at Order Schedule 4 (Order Tender);
"Other Contracting Authority"	any actual or potential Buyer under the DPS Contract;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted by Law;
"Party"	in the context of the DPS Contract, CCS or the Supplier, and in the in the context of an Order Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits;

"Performance Indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the DPS Contract set out in DPS Schedule 4 (DPS Management);
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;
"Personnel"	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract;
"Platform"	the online application operated on behalf of CCS to facilitate the technical operation of the DPS;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies;
"Processing"	has the meaning given to it in the GDPR;
"Processor"	has the meaning given to it in the GDPR;
"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;
"Progress Report Frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
"Prohibited Acts"	a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for

	improper performance of a relevant function or activity in connection with each Contract; or c) committing any offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;
"Protective Measures"	appropriate technical and organisational measures which may include pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in DPS Schedule 9 (Cyber Essentials), if applicable, in the case of the DPS Contract or Order Schedule 9 (Security), if applicable, in the case of an Order Contract;
"Recall"	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	the Supplier's plan (or revised plan) to rectify its breach using the template in Joint Schedule 10 (Rectification Plan Template)which shall include: a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
"Rectification Plan Process"	the process set out in Clause 10.4.3 to 10.4.5 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);

"Reimbursable Expenses"	the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential Information"	a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR); b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and information derived from any of the above;
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
"Reminder Notice"	a notice sent in accordance with Clause 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Order Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;

"Request For Information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
"Schedules"	any attachment to a DPS or Order Contract which contains important information specific to each aspect of buying and selling;
"Sectors and Domains"	the Sectors and Domains Filter Category defined in DPS Schedule 1;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Order Schedule 9 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Self Audit Certificate"	means the certificate in the form as set out in DPS Schedule 8 (Self Audit Certificate);
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Order Contract (which, where Order Schedule 14 (Service Credits) is used in this Contract, are specified in the Annex to Part A of such Schedule);
"Service Period"	has the meaning given to it in the Order Form;
"Services"	services made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Service Type"	means the Service Types Filter Category detailed in DPS Schedule 1
"Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;

"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
"Special Terms"	any additional Clauses set out in the DPS Appointment Form or Order Form which shall form part of the respective Contract;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in DPS Schedule 1 (Specification), as may, in relation to an Order Contract, be supplemented by the Order Form;
"Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in DPS Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; d) relevant Government codes of practice and guidance applicable from time to time;
"Start Date"	in the case of the DPS Contract, the date specified on the DPS Appointment Form, and in the case of an Order Contract, the date specified in the Order Form;
"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Order Procedure;
"Storage Media"	the part of any device that is capable of storing and retrieving data;

"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than an Order Contract or the DPS Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Supplier"	the person, firm or company identified in the DPS Appointment Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Order Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the DPS Appointment Form, or later defined in an Order Contract;
"Supplier's Confidential Information"	a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Order Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Order Contract;
"Supplier Non-Performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or

	c) comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of an Order Contract for the relevant period;
"Supplier Profit Margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"Supply Chain Information Report Template"	the document at Annex 1 of Joint Schedule 12 (Supply Chain Visibility);
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Order Contract detailed in the information are properly payable;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;
"Test"	any test required to be carried out pursuant to the Order Contract i) as set out in the Test Plan agreed pursuant to Part B of Order Schedule 13, ii) or as specified elsewhere in this Order Contract, and "Testing" and "Tested" shall be construed accordingly;
"Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
"Transparency Information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and (ii) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Order Schedule 1 (Transparency Reports);

"US-EU Privacy Shield Register"	a list of companies maintained by the United States of America Department for Commence that have self-certified their commitment to adhere to the European legislation relating to the processing of personal data to non-EU countries which is available online at: https://www.privacyshield.gov/list;
"Variation"	has the meaning given to it in Clause 24 (Changing the contract);
"Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and
"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form.

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	**[delete** as applicable: CCS / Buyer**]** ("**CCS" "the Buyer"**) And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete** as applicable: CCS / Buyer**]**

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature [redacted]

Date .....

Name (in Capitals) .....

Address .....

.....

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under an Order Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the DPS Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Order Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if you aren't insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in

dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following standard insurance cover from the DPS Start Date in accordance with this Schedule:

1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000);

1.2 public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than five million pounds (£5,000,000); and

1.3 employer's liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)

1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

3.1 The Supplier:

3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world.

3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world.

3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;

3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

4.1.1 ensure that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;

4.1.3 ensure that all workers are provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;

5.1.2 ensure that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;

5.1.3 ensure that use of overtime is used responsibly, taking into account:

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

5.3.1 this is allowed by national law;

5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

5.3.3 appropriate safeguards are taken to protect the workers' health and safety; and

5.3.4 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

6. Sustainability

6.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Supplier is entitled to sub-contract its obligations under the DPS Contract to the Key Subcontractors identified on the Platform.

1.2 The Supplier is entitled to sub-contract its obligations under an Order Contract to Key Subcontractors listed on the Platform who are specifically nominated in the Order Form.

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

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

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

1.3.3 the proposed Key Subcontractor employs unfit persons.

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

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

1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

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

1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected DPS Price over the DPS Contract Period;

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

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

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

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

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

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

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

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

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

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

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

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

(c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

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

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

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

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

Joint Schedule 7 (Financial Difficulties)

1. Definitions

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

"Credit Rating Threshold"	the minimum credit rating level for the Monitored Company as set out in the third Column of the table at Annex 2 and
"Financial Distress Event"	the occurrence or one or more of the following events: a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; d) Monitored Company committing a material breach of covenant to its lenders; e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or f) any of the following: i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract; ii) non-payment by the Monitored Company of any financial indebtedness;

	iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Order Contract;
"Financial Distress Service Continuity Plan"	a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with each Order Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	Supplier [the DPS Guarantor/ [and Order Guarantor] or any Key Subcontractor]
"Rating Agency"	the rating agency stated in Annex 1.

2. When this Schedule applies

2.1 The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Schedule shall survive termination or expiry of this Contract.

3. What happens when your credit rating changes

3.1 The Supplier warrants and represents to CCS that as at the Start Date the credit rating issued for the Monitored Companies by the Rating Agency is as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within ten (10) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by the Rating Agency for a Monitored Company which means that the credit rating for the Monitored company falls below the Credit Rating Threshold.

3.3 If there is any such downgrade credit rating issued by the Rating Agency for a Monitored Company the Supplier shall at CCS' request ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

3.4 The Supplier shall:

3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agency; and

3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if the Rating Agency has rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. What happens if there is a financial distress event

4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.

4.3 The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1 at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2 where CCS reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

(a) submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and

(b) provide such financial information relating to the Monitored Company as CCS may reasonably require.

4.4 If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

4.5 If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

4.6 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;

4.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

4.6.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.

4.8 CCS shall be able to share any information it receives from the Supplier in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

5. When CCS or the Buyer can terminate for financial distress

5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

5.1.3 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

6. What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agency reviews and reports subsequently that the credit rating does not drop below the relevant Credit Rating Threshold, then:

6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default:	[**Guidance:** Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the [Revised] Rectification Plan:	[**add** date (minimum 10 days from request)]		
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default	[**add** cause]		
Anticipated impact assessment:	[**add** impact]		
Actual effect of Default:	[**add** effect]		
Steps to be taken to rectification:	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[**add** reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Status of the Controller

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

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

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

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

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

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

Where one Party is Controller and the other Party its Processor

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

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

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

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

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

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

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

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

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it

is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

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

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

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

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

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

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

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

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

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

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

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

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound,

uses its best endeavours to assist the Controller in meeting its obligations); and

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

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

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

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

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

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

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

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

(f) becomes aware of a Data Loss Event.

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

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

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

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

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

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

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

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

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

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

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

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

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

12. Before allowing any Sub-processor to Process any Personal Data related to the Contract, the Processor must:

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

(b) obtain the written consent of the Controller;

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

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

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

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

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

Where the Parties are Joint Controllers of Personal Data

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

Independent Controllers of Personal Data

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

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

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

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

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

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

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

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

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

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

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

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

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

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

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

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

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

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

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

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

26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data A) Template

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

1.1 The contact details of the Relevant Authority's Data Protection Officer are: [redacted] nhsdigital.dpo@nhs.net

1.2 The contact details of the Supplier's Data Protection Officer are: [redacted] – dataprivacy@kpmg.co.uk

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

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

For the avoidance of doubt, access to personal data is not expected to be generally necessary for the scope of the Services outlined in this Contract and the Order Form, and the Supplier Personnel shall not generally have access to any personal data of NHS England. However, it is recognised that on occasion it may become necessary for NHS England to require services associated, where the Supplier will be given access to personal data. Where any such service request gives access to personal data, the Supplier shall access such data as processor to NHS England, and the following table shall apply (as updated where necessary in the agreed SOW).

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: • ***[Insert** the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer]* **The Supplier is Controller and the Buyer is Processor** *The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:* • ***[Insert** the scope of Personal Data which the purposes and means of the Processing by the Buyer is determined by the Supplier]* **The Parties are Joint Controllers** *The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:* • ***[Insert** the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]* **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:*

	• *Business contact details of Supplier Personnel for which the Supplier is the Controller,* • *Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller,* • ***[Insert** the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer]* ***[Guidance** where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]*
Duration of the Processing	*[Clearly set out the duration of the Processing including dates]*
Nature and purposes of the Processing	*[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular* *website etc]*

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]*

B) DPS Contract Personal Data Processing

Description	Details
Identity of Controller for each Category of Personal Data	**CCS is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 and for the purposes of the Data Protection Legislation, CCS is the Controller and the Supplier is the Processor of the Personal Data recorded below
Duration of the Processing	Up to 7 years after the expiry or termination of the DPS Contract
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this DPS Contract including i. Ensuring effective communication between the Supplier and CSS ii. Maintaining full and accurate records of every Order Contract arising under the Framework Agreement in accordance with Core Terms Clause 15 (Record Keeping and Reporting)
Type of Personal Data	Includes: i. Contact details of, and communications with, CSS staff concerned with management of the DPS Contract ii. Contact details of, and communications with, Buyer staff concerned with award and management of Order Contracts awarded under the DPS Contract, iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract Contact details, and communications with Supplier staff concerned with management of the DPS Contract

Categories of Data Subject	Includes: i. CSS staff concerned with management of the DPS Contract ii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the DPS Contract iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract Supplier staff concerned with fulfilment of the Supplier's obligations arising under this DPS Contract
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	All relevant data to be deleted 7 years after the expiry or termination of this DPS Contract unless longer retention is required by Law or the terms of any Order Contract arising hereunder

Annex 2 - Joint Controller Agreement

Not Applicable

Order Schedule 1 (Transparency Reports)

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

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

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

4. The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Performance Metrics	Summary of Services by SOW provided for each month during the preceding Quarter.	MS Word or Excel	Quarterly
Order Contract Charges	Summary Charges under the Call Off Contract for the preceding quarter	MS Word or Excel	Quarterly
Key Subcontractors	Key Sub-Contractors utilised in the contract, including proportion of Call Off Contract Charges spent with sub-contractors	MS Word or Excel	Quarterly
Performance management	Breakdown of resources used in delivery of the Services over the duration including: - Roles Grade Days utilised	MS Word or Excel	Monthly

Order Schedule 6 (ICT Services)

1. Definitions

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

"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Order Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Commercial off the shelf Software" or "COTS Software"	non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms;
"Defect"	any of the following: a) any error, damage or defect in the manufacturing of a Deliverable; or b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract; or d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality

	specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract;
"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Order Contract, including any COTS Software;
"New Release"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or c) where any part of the Supplier System is situated;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Order Schedule shall also include any premises from,

	to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 8.1 of this Schedule;
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT services which are part of the Deliverables.

3. Buyer due diligence requirements

3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2. operating processes and procedures and the working methods of the Buyer;

3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2. The Supplier confirms that it has advised the Buyer in writing of:

3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the Deliverables;

3.2.2. the actions needed to remedy each such unsuitable aspect; and

3.2.3. a timetable for and the costs of those actions.

4. Software warranty

4.1. The Supplier represents and warrants that:

4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Order Contract including the receipt of the Deliverables by the Buyer;

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications and Documentation; and

4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

5.1. The Supplier shall:

5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with any interface requirements of the Buyer specified in this Order Contract and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.1.3. ensure that the Supplier System will be free of all encumbrances;

5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Order Contract;

5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

6.1. The Supplier shall, where specified by the Buyer as part of their Order Procedure, and in accordance with agreed timescales, develop quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").

6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Order Contract Period:

6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Order Contract;

6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

7.1. The Supplier shall allow any auditor access to the Supplier premises to:

7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Intellectual Property Rights in ICT

8.1. **Assignments granted by the Supplier: Specially Written Software**

8.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

8.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

8.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

8.1.2. The Supplier shall:

8.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

8.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan,

achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

8.1.2.3. without prejudice to paragraph 8.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

8.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

8.2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**

8.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

a) of its own Existing IPR that is not COTS Software;

b) third party software that is not COTS Software

8.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Order Contract Period and after expiry of the Order Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

8.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to

the Buyer on terms at least equivalent to those set out in Paragraph 8.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

8.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

8.2.3.2. only use such third party IPR as referred to at paragraph 8.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

8.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 8.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

8.2.5. The Supplier may terminate a licence granted under paragraph 8.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

8.3. **Licenses for COTS Software by the Supplier and third parties to the Buyer**

8.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

8.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

8.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 8.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

8.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

8.3.4.1. will no longer be maintained or supported by the developer; or

8.3.4.2. will no longer be made commercially available

8.4. **Buyer's right to assign/novate licences**

8.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 8.2 (to:

8.4.1.1. a Central Government Body; or

8.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

8.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 8.2.

8.5. **Licence granted by the Buyer**

8.5.1. The Buyer grants to the Supplier a licence to use the Specially Written Software i) during the Order Contract Period for the purpose of fulfilling its obligations under the Order Contract, and ii) after the Contract period on the terms set out in the Open Government Licence.

8.5.2. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

8.6. **Open Source Publication**

8.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 8.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

8.6.1.1. suitable for publication by the Buyer as Open Source; and

8.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

8.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

8.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

8.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

8.6.2.3. do not contain any material which would bring the Buyer into disrepute;

8.6.2.4. can be published as Open Source without breaching the rights of any third party;

8.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and

8.6.2.6. do not contain any Malicious Software.

8.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

8.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

8.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9. Supplier-Furnished Terms

9.1. Software Licence Terms

9.1.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 8.2.3 are detailed in Annex A of this Order Schedule 6.

9.1.1.2. Terms for licensing of COTS software in accordance with Paragraph 8.3 are detailed in Annex B of this Order Schedule 6.

ANNEX A

Non-COTS Third Party Software Licensing Terms

Not Applicable

ANNEX B

COTS Licensing Terms

Not Applicable

Order Schedule 7 (Key Supplier Staff)

1. The Annex 1 to this Schedule lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

2. The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

3. The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

4. The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

   4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

   4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

   4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

5. The Supplier shall:

   5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

   5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

   5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least 1 Months' notice;

   5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

6. The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Order Schedule 8 (Business Continuity and Disaster Recovery)

1. BCDR PLAN

1.1 At the Supplier's request, the Customer shall provide the Supplier with a copy of its Business Continuity & Disaster Recovery ("BCDR") Plan.

1.2 The Supplier shall develop a BCDR Plan and ensure that it is linked and integrated with the Buyer's BCDR Plan and the Supplier shall review and amend its BCDR Plan on a regular basis and as soon as is reasonably practicable on receipt of an amended Buyer BCDR Plan from the Buyer.

1.3 The Supplier shall ensure that its Sub-Contractor's BCDR Plans are integrated with the Supplier's BCDR Plan.

1.4 If there is a Disaster, the Parties shall, where applicable, implement their respective BCDR Plans and use all reasonable endeavours to re-establish their capacity to fully perform their obligations under this Order Contract. A Disaster will only relieve a Party of its obligations to the extent it constitutes a Force Majeure Event in accordance with Clause 20 (Circumstances Beyond Your Control).

Order Schedule 9 (Security)

Part B: Long Form Security Requirements

1. Definitions

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

"Breach of Security"	means the occurrence of: a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
"ISMS"	the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
"Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

2.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.3.1 [redacted] security representative of the Buyer

2.3.2 [redacted] security representative of the Supplier

2.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

3.3.1 If the Buyer has not stipulated during an Order Procedure that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.3 at all times provide a level of security which:

(a) is in accordance with the Law and this Contract;

(b) complies with the Baseline Security Requirements;

(c) as a minimum demonstrates Good Industry Practice;

(d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

(e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)(https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

(f) takes account of guidance issued by the Centre for Protection of National Infrastructure https://www.cpni.gov.uk/

(g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

(h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

(i) addresses issues of incompatibility with the Supplier's own organisational security policies; and

(j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph

4.3 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those

incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex nnex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

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

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the

Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 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 Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, 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 Buyer) necessary to:

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

(b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

(c) apply a tested mitigation against any such Breach of Security 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 provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

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

(e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

(f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the

requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for 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 ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

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

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (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 a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 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 Buyer; or

9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation

techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

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

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.4.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) 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;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 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 ICT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

8.1 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:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

Not Applicable at this stage

BUYER'S SECURITY POLICY

Information Security Policy (1).pdf

Order Schedule 15 (Order Contract Management)

1. Definitions

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

"Operational Board"	the board established in accordance with paragraph 5.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be the delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Contract Risk Management

4.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Order Contract.

4.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

4.2.1 the identification and management of risks;

4.2.2 the identification and management of issues; and

4.2.3 monitoring and controlling project plans.

4.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

4.4 The Supplier will maintain a risk register of the risks relating to the Order Contract which the Buyer and the Supplier have identified.

5. ROLE OF THE OPERATIONAL BOARD

5.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

5.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

5.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

5.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

5.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Meeting	Frequency	Agenda	Supplier Representative	NHSE Representative
Operational Board/Account Meeting	Quarterly	Review overall contractual performance and feedback on meeting contract needs • Strategic discussions e.g Continuous Improvement. Future work		Programme SRO/Lead Requester Commercial Representative
Monthly SOW performance/pipeline	Monthly	Review of SOW performance / pipeline/issues/		Programme SRO/Lead(s) Requester
Project/SOW Review	As and when SOW's are commissioned	Review SOW deliverables, issues, and risks.		Programme SRO/Lead(s) Requester

Order Schedule 20 (Order Specification)

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

OVERARCHING CALL OFF CONTRACT – SERVICE REQUIREMENTS

Bid pack

Table of Contents

1. Purpose

1. Cyber security is a strategic priority across Government. A series of key national documents have been published over the past three years, including two Integrated Reviews, National and Government Cyber Security Strategies and our own Cyber Strategy for Health and Care to 2030

2. The Governments Cyber Security Strategy to 2030 sets out the criticality of building and maintaining our nation's cyber defences. The Data Saves Lives strategy sets out plans to harness digital efficiency and data to improve outcomes, while maintaining the highest standards of privacy and ethics and taking targeted action to build public trust around how we use data in the NHS. This sits alongside the Plan for Digital Health and Social Care, which sets out a vision and action plan to digitise health and care services and connect them to support integration, using this platform to transform, enabling fundamentally new care models.

3. The Cyber Improvement Programme

The Cyber Improvement Programme[1] is aimed at supporting the Health and Care Sector to continue to adapt and improve its cyber resilience against the evolving threats, protect itself and retain public confidence. The health and social care sector resist cyber threats every day, including:

(1) phishing and other malicious emails,
(2) automated scanningifor common software vulnerabilities and
(3) attempted fraud.

All these threats pose risks not just to patient and staff safety, but also to public trust in a health and social care system that can and must safeguard people's data.

4. NHS England is seeking a Cyber Partner to provide subject matter expertise across its security estate that will cover a breadth of areas within the Organisation, including Estates Visibility, Cyber System Risk Management and Data, Response & Recovery, Standards, Policy and Guidance, Supply Chain Management, System Support & Investment and System Workforce which are all part of the Cyber Improvement Programme.

5. The Provider will have significant experience in the shaping of cyber functions and capabilities and will bring understanding of industry trends and best practice, to help define the strategies and policies that will align to the Cyber Improvements Programme and to the aspirations of the Health and Care Cyber Strategy to 2030.

[1] A cyber resilient health and adult social care system in England: cyber security strategy to 2030 - GOV.UK (www.gov.uk)

2. Overarching Call Off Contract

2.1 The Buyer will require the provision of a range of services throughout the duration of the contract, this section reflects the likely needs of the Buyer for future Statement of Works.. The types of skills and capabilities required from the Provider during the term of the contract are in four broad areas:

- Cyber specialists who can help shape and create strategy / policy (and governance) outputs.
- Cyber specialists with an understanding of cyber security at an operational level to help build and establish new products, services, and capabilities.
- Cyber specialists with a detailed knowledge of technologies and processes for example, Microsoft Sentinel, Microsoft Defender for Endpoint, ELK, Microsoft Azure, as well as a detailed operational knowledge of specific cyber processes such as Incident Management, Threat Intelligence, Threat Hunting, Threat Monitoring, Penetration testing, Continuous testing, DevSecOps. In addition, ability to incorporate cyber knowledge into areas such as cyber risk, incident management and estate visibility will be required.
- Technical and other specialists who can implement and establish change for example, user researchers and service management with cyber knowledge.

Below are the likely themes of support that will be needed for these services. This will not be a totally comprehensive list but broadly demonstrates the areas of expertise needed.

Security Architecture and Solution Architecture	User Research - Cyber	CSOC/Live Services SME	Service Management Specialists & Change Management	Service Design and UX
Risk Management / Cyber Security Risk and Assessment	Attack Surface Management implementation	MOE Dashboard SME (Data scientists]	Cross Systems Cyber Expertise	Incident Management

3rd Party Supply Chain Risk				
Cyber Data & Analytical	MS Defender Subject Matter Experts	Market Research SME	Cyber Policy/Governance Privacy, Transparency and Ethics (PTE)	Control and Compliance

2.2 The Provider will be expected to deliver several wornk packages as they are formed throughourt the term of the contract.. This will be in the form of a call off model explained under section 7 "the Commissioning Process". Detailed requirements for the first 3 SOW's /Work pa.ckages can be found at section 6 of this document.

2.3 Future Cyber work packages covering1cyber focused outputs willl be spread across 8 workstreams including.

- Estates Visibility- the workstream focus iis to increase estate visiibility through increased adoptiion/ feature enablement of the centra.lly funded Microsoft Defender product sets (servers, end points, IoT/Med Devices) with additional support to promote uptake/ usage and the provision of dashboards to support better reporting and exploitation of the data as welll as external attack surface visibility.

- Cyber System Risk Management and Data - the workstream focus is to define the risk manag1ement lifecyde, delliver a change in culture across the wider Cy'ber Operations and programme team, to drive future direction and decision making throughthe risk management lifecycle, develop and deploy a cyber risk data platform and to deliver governance, risk, and compliance traiining..

- CSOC Enhancements - the workstream focus is to deliver the followiing CSOC capabiliities and enhancements:

    - Managed Securiity Service Provider {MSSIP) - deliiver a nationallly provided MSSP using an enhanced serviice model that interfaces with Hea.lth and Sociial Care, Primary and Secondary Care and Arm's length bodies..
    - Multi Tenancy Monitoring (MTM)
    - NHSmail - deliver an enhanced monitoring archiitecture and service design to enable NHSmail platform to be fully monitored by NHS

England Central Security Operations Centre.
- Deployment of]hreat Intelllligence Platform (TIP)
- Operational Data Platform (ODP) - improve the capability of protective monitoring with a unified data source through the consollidation of large disparate datasets through one interface to enable threat hunting, trends anallysis, and investig1ation of suspicious activi Y-
- Microsoft Baseline Tooling - migration to Miicrosoft Sentinel

- Response & Recovery- the workstream focus is on establishing1 excellent, well documented national cyber incident response processes and plans, production of an exercise strategy to ensure plans are well embedded across NHSE and DHSC organisations, tested and improved, creation of best practice guidance for hea.lth and care providers in inciident manag1ement response to improve local and regional capability. Also, the worikstream wiill scale up NHSE's cyber exercising offer to system partners to ensure plans are well rehearsed and undertake a diiscovel)I work into a recommended lncident Response (IR) traiining course, standard or certification, contextualised for the health and care landscape.

- Standards and Policy Guidance - the focus of this worlkstrearn is to create processes and structure to define the requirements for supporting documentation to reduce cylber risk, induding by exploring what documentation is available now as well as defining What is needed in addition; the management of the life cycle of all standards, policiies and guidance including create/approve method through collaborative workiing1 groups. This also includes the creation of a corpus of policy and g1uidance documentation to support organisations as cyber improvement programme is deliivered, development of a framework to deliver and exploit the strategic commitment to adopt the CAF as the basis of the DSIPT and the devellopment of a complliance and assurance framework.

- Supply Chain Manag1ement - the worikstream focus is to design and define a single methodology and criiteria to enable the health and care system to consistentl'y identify critical services, systems, and technologies, define requirements for a national supplier management platform alongside clear guidance of a supplier definition and to develop a risk assurance model for supplier assurance together with security schedules, to be used duriing1and after product, services, and software procurement.

- System Support & Investment - the workstream focus iis on the stratification of providers, development of engagement and capital spend strategiy, identification of candidates for exemplars and enforcement and to develop artefacts and templates for risk reduction.

- System Workforce - develop the cyber workforce capabilitiies/strategy through the development of a library of evaluated job descriptions, support, package for the integrated care systems and a plan for development and iimplementation of a talent pipeline. This also involves the development of the target operating model development of each cyber professiional competency profile, career and development pathways, the development of a cylber school and a culture/role modelling for the cyber professiion.

2.4 The Provider will also support the deliverables of the internal NHS England risk reduction programme, to reduce the securiity misk and improve resilience of NHS Englland's systems and services, including those that are classiified as Critiical National !Infrastructure (CNI).

2.5 The Provider may be required to establiish new technologies, build and refine processes, and particiipate in training. The Statement of works will define the capabilities required for the delivery of the work packages.

2.6 Potential Providers should note that there willlbe several procurement opportunities published in support of the Cyber Improvement Programme. These will reference the workstreams highlighted in 2..3. lit is important to note that the work for this Provider focusses on cyber specialism required for the Progiramme and other procurements will have other primary focus areas.

Expectations and defining competency in Cyiber Security	**Required Aggregate Team Experience**
Cyber Estates/ Cylber System Management and Data within a large-scale data services org1anisation and operational service domain	10 years
Assessment, pllanning, risk management encompassing all ell-ements requiired in the design of Cyber Standards and Policy Guidance	10 years
The management of Cyber rellated large-scale operational transformations.	10 years
Progiramme level g:ovemance and assurance within a large-scalle complex Cylber environment	10 years
Please note that this is *the minimum and individual work packages may require specific capabilities and skills..*	

2.7 The Buyer is seeking a Partner for the Cyber Improvement Programme iinitially from **1** Aprill 2024 to 31 March 2027 based on a 3-year call off contract (with options to extend 2 x 12 months) to deliver the required work packages.

2.8 The overall contract value is capped at [redacted] with annual break points to review.

2.9 The Order Contract is non-excllusive, and the Buyer cannot guarantee volumes of work as part of this Contract.

2.10 As this programme is aimed at delivering strategiic objectives across the health and care system, the provider wou1ld ideally have a good understanding of the NHS and the health and care system.

3. Background to the contracting authority

The Cyber Improvement Programme iis aimed at supporting the health and care sector to continue to adapt and improve its cyber resilience agaiinst the evolving threats, protect itself and retain public confidence. The programme will help partner with regional leads/ teams that understand the system where appropriate taking a collaborative approach towards achieving the common goal of reducing cyber risk.

The aims and objectives of the programme are:
S01: - Minimising the impact of cyber security incidents -To Improve the ability of the hea.lth and care system to effectively respond to cybersecurity incidents, where they do occur, to minimise impact on patient care.

S02: - Increased cyber economies of scale- to create cost effective cyber security detection by provision of national CSOC products and services, thereby reducing duplication of spending in ICSs and providers. This can be evaluated by an increase in uptalke of national cyber security products and services by a median of [redacted] by 2025.

S03: Increase Efficiency - to make better use of new and existing cyber security solutions through provision of standardised national products and services, creating more efficient and standardised cyber processes leading to a better cyber risk evidence base for the futiure. This can be evaluated by an increase in uptake of national cyber security products and services by a median of [redacted] by 2025.

S04I: Increase Gompliiance - to increase the proportion of organisations who are compliant with **the** newly defined national cyber standards for health and social care. This can be quantified by 100% compliance of 'Must Do' DSPT measures across all Cat 1 organisations (ICSs and NHS trusts) by 2025.

The health and care organisations that the Cyber Improvement Programme work with are:

- NHS England National
- NHS England Regions
- ICSs with responsibility to ICBs
- Primary Care Providers
- Secondary Care Providers
- Adullt Social Care Providers
- Critical !National Infrastructure
- Supply Chain
- Arm's Length Bodies

4. Background to requiremenUoverviiew of requiirement

The health and care sector iis required to deliiver high-quality patient care while maintaiining the confidentiality, iintegrity, and availabiility of critical healthcare data and systems.

There are insufficient cyber capabiliities and expertise available internally within NHSE to complete the deliverables of the Cyber Improvement Programme hence the engagement of a Provider is requirred to meet the Programme's tight timelines and deliverables.
Some of the team members are redirected to incident response and otherrlive service priorities which impacts on their availability to support the Cyber Improvement Programme in terms of meetiing the objectives within the planned milestones.

The high-level list of deliverables for the programme include (not in chronological order):

- Risk quantification and Libraries of Scenarios - This indudes development of a threat actor library, devellopment of key **risk** scenarios and associiated risks, assessment of risks for impact/likellihood, quantificatiion of risks based on assumed data, Natiionall baseline quantificatiion of risk through interviews with a widle range of stakeholders, attack tree developmenUanalysis and response development and Cyber data baseline development and analysis.

- Estate Visibility Strategy - Increase asset visibility by expanding and explloiting use of existing centrally funded product sets as well as

extending coverage. Make available asset data to the system locally, regionally, and nationally and refine/deliver the defender roadmaps and produce estate visiibility dashboards..

- MOE Extended Deployment - extend the deployment of Microsoft Defender for Endpoint across the health and care system.
- MOE Reporting/ Roadmap - define the roadmap for the deployment of MOE and definition of reporting requirements for MDE deployment.
- Multi-Tenancy Operations - Deployment of multi-tenancy monitoring (MTM} serviices to Health and Social Care org1anisations to enable CSOC to monitor organisations with an Azure tenant (including AILBs) and Microsoft 365 Defender Instances.
- NHSMail Monitoring - Ingest NHSMail into CSOC Infrastructure and operating processes.
- Threat Intelligence Platform - Deployment of NHSE CSOC Threat Intellligence (TI} to organisations in health and social care.
- Operational Data Platform - Deployment of a big data solution to enable CSOC to leverage multiple datasets through one interface, threat hunt, anallyse trends and investigate suspicious activity.
- System Engagement Modelliing and Stratification - Development of a Cyber Improvement communication, marketing and engagement model and an organisational stratifiication model and associated collateral to proviide local organisations with a current state view and defined roadmap for improvement..
- System Support Model - devellopment of a siimplified cyber-service model and dear routes of a.ccess to support.
- Strategic System Investment - development of a strategic iinvestment process and high-level pllan based on a series of agreed principles, previious investments and lessons learned.
- ICS Cyber Strateg1iies - Provide support for local ICSs to develop and own their cyber strategies.
- Policy, Standards, Guidance, and Process Repository - Development of policy, standards and guidance includiing repository for their management.
- DSPT/CAF Redevelopment - Redevellopment of DSPT *to* use the Cyber Assessment Framework.

- Compliance and Assurance framework - Develop compliancy framework linking with DSPT and GAF to develop a sustainable assessment framework.

- Supplier Risk Assurance - Identification of critical suppliers and development of a framework and model for defining supplier risk assuirance and accountabilities.
- Supplier Cyber Security clause - standardisation of supplier cyber secuirity terms and conditions provisions into the NHS Standard Contract and all NHS endorsed commercial framework.

- !Response Planning and training - Develop excellllent, well documented national! cyber incident response processes and plans, produce an exercise strategy to ensure plans are well embedded across INHSE and DHSC organisations, tested and improved, create best practice guidance for health and care providers in incident management response to improve local and regional capability, scale up NHSE's cylber exercising offer to system partners to ensure plans are well rehearsed and discovery into a recommended Incident Response (IR) training course, standard or certification, contextualiised for the health and care landscape.

- IRed team playbook (with inclusion of purple team) - Development of a playboolk including1rules of engagement for exercising and creation of templates and artefacts and delivery of a testing and exercising plan including purple teaming.

- Development of standardisation to meet security requirements.

5. Definitions

Expression or Acronym	Definition
MTM	Multi Tenancy Monitoring
SO	Spending Objectives
CSOC	Central Security Operations Centre
ODP	Operational Data Platform
ELK	ElasticSearch, Loqstach and Kibana
SOW	Statement of Work- each piece of work identified will be called off usinq the SOW template
Commissioning Process	The process guidance of how SOW's will be commissioned.

6. Scope of requirement

6.1 The mandatory requirements are specified in the high-level requiirements document located in the standard qualification sectiion of the ITT. Thiis is a pass/faiil section, and all potentiial bidders must confirm they can fully meet all described elements.

6..2 The mandatory requirements will apply to all the work packages that will be delivered by the provider throughout the duration of the calll-off contract.

The requirement - SOW's

6.3 The Cyber Improvement programme will adopt a call-off model to deliver different work packages across the various workstreams. The first work package that the provider will be expected to deliver willl be as per the milestone delivery tables and are described in SOWs 1 -3:

SOW 1 - CSOC Future State Design

The NHS Cyber Security Operations Centre (CSOC) iis responsible for providing protective monitoring1services aciross the health and care system. As part of its mandate the CSOC monitors a diverse set of health and care systems/services, including NHS National Services (critical services which underpin the NHS). The CSOC is responsible for ensuring tlhe confiidentiallity, integrity, and availlabiility of these assets by monitoring malicious activities, identifying, and managing1incidents..

The CSOC consists of the following operational teams:

- SecOps: moniforing and triage of secuirity alerts and incidents.
- DevOps: onboarding andl tuning of services.
- ThreatOps: Specialist, threat-led capabilities to enhance secuirity posture, monitoring, and response.
- ServiceOps: reportingi and tracking of services being monitored.
- Incident Management management of incidents.

The CSOC work package deliverables :
Development of material to support the delivery of the CSOC Future State Design, Strategy, Roadmap and Service Catalogue to support the Health and Care System and help the holistic mitig1ation of cyber risk at scale.

The key outputs of the delivery are:

1. Fully documented and agreed stakeholder register (in-line with NHSE standards)

2. Fully documented Analysis of stakeholders (in-line with NHSE standards).
3. Identification, analysis, validation, and documentation of previous analytical work..
4. Elicitation, analysis, validation Agreed/ Sigined off user needs register/ requirements catalogue for all key stakeholder groups.
5. Documented analysis of external/ internal factors that will impact the future state design CSOC strategy (using common analysis frameworks such as 'SWOT'/ 'PESTLE / etc.).
6. Documented/ agreed analysis of the role of the National CSOC in the National Cyber TOM

Milestone/Delliverable	Deliverables/Taslks	Timeframe or Deliverv Date
Initiation Meetingi& Scoping	An initial meeting between Buyer and Supplier to g1ain additional information and context regarding the Buyers organisation and to further clarifv the scooe.	Within week 1 of Contract Award
(1&2) Stalkeholder Identificatiion, Analysiis and Documentatiion	This activity will cover all Health and Care Organisations, as previously defined earlier in this document. The dellivernble associated to this work is a stakeholder analysis that can be used to outline the scope of stakeholder engagement/ interest in future activities.	Withiin 2 weeks
Identification, analysis, validation, and documentation of previous analytical work..	Work with the buyer to identify previous work that can be used to feed / re-used to assist in the development of the CSOC future state design, strateg1y, roadmap, and service catalooue.	Withiin 4 weeks
4. Documented anallysis of external / internal factors that will impact the future state design CSOC strategy	Using existing material as well as the Suppliers extensive cyber {global) knowledge	Within 6 weeks, as well as the cy'ber-SMEs from within NHSE and other national bodies (NCSC), create an analysis of internal / external! factors that should be taken into consideration when developing the CSOC Future State Design and Strategy.

Eliciitatiion, analysiis, validation Agreed/ Signed off user ne,eds register / requirements catalogue for all key stakeholder groups.	The output of this activity is an agreed set of user needs from key stakeholders - it is recognised that this won't be a fully agreed catalogue of user needs from all stakeholders, it is critical that the stakeholders iidentified in the previous analysis as high influence/high power are prioritised dn aqreement with the Buyer).	within 8 weeks (to be undertaken in parallel with other tasks
Documented/ agreed analysis of the rolle of the National CSOC in the National Cyber TOM	An agreed document that adds iurther analysis/ understanding to the role the CSOC will play within the National Target Operating Model, this task will involve the analysis of the System wide TOM {in development) and discussion with Cyber SMEs from NHSE and other National bodies.	within 8 weeks.

SOW 2 - Cyber **Risk** Reduction

1. The programme requires support to develop a service catalogue and associated artefacts, policy, process, procedure aligned to relevant frameworks and standards with key output being the Pen Test Pollicy & Standards to align to DSIPT, CAF, ISO27001, Full Penetration Testing Service catalogue, with detailed descriptions.

2. The programme requires support to develop a playbook includingirules of engagement for exercising and creation of templates and artefacts and the delivery of a testing and exercising1plan indu:ding1purple teaming. The Key Output of this will be red team playbook and plan, and purple teaming.

3. The programme requires support to develop a research paper on the benefits, limitations and options of continuous testing and penetration testing and how it could be implemented within the enterprise.

4. The Provider will support the programme to consolidate the secu1riity requirement from existing security controls catalogue into a set of key compliance questions that can be aslked of programmes/product/systems owners to capture security compliance information. The key output will be development of a compliance question set for programmes/product/systems owners to assess security compliance information.

5. Develop a Security Policy Framework (including Policy Governance & Working Group) - This iis aiimed at unifying the security policy governance, supportiing the delivery of a new security strategy for the newly merged organisation. The lkey output will be the security pollicy framework.

Milestone/Deliverable	Deliverables/Tasks	Timerrame or Delivery Date (indicative)
Initiation Meeting & Scoping	An iniitial meeting between Buyer and Supplier to gain additional information and context regarding the Buyers organisation and to further darify the scope.	Within week 1 of Contract Award
Engagement activities for the development of a service catalog1ue and associated artefacts, policy, process, procedure etc	Engagement with Cyber Ops team and other team outside of Cyber Ops (e.g., ServiiceNow team, Buyers) to define / vallidate the artefacts	Within 2 weeks
Develop service catalog1ues, artefacts, poliicy, process, and procedure documents	1 Service catalogue 1 Policy document 1 standards document 1 Procedure document	Within 4 weeks
Develop compliance question set	The compliance question set will be used to assess the following: 1. Progiramme owners 2. Product owners 3. Serviice owners/System/Asset Owners 4. Developers	Within 5 weeks
Quality checks of the deliiverables	Deliverables to be signed off by rellevant member of the CISO team (functional heads - i.e., Secure, Assure, GRC)	Within 6 weeks

SOW 3 - **DSPT Audiit**

The Key outcomes to the delivery of this statement of work are as follows:

1. . Reuse the existing DSPT framework (Data Security and Protection Toolkit (dsptoolkit.nhs.uk)) and repurpose it for CAF-aligned DSPT (Category 1 including Trusts NHS Trusts, ALBs, CSUs and ICBs) from the existing 10 National Data Guardian standards to the heallth-based objectives aligned to the CAF /principles. NCSC CAF principles and guidance - NCSC.GOV.UK.
2. . Test the outcomes of the new GAF-aligned DSPT framework using 5 Volunteer or faux audits provided by NHS England team and update the framework wiith the lessons learnt from testing the outcomes.

3. Conduct 5 audits {of organisations provided by NHS England) post-go live of the New CAF audit framework and participate in an improvement cycle.
4. Develop Thematic report following post-910 live audits.
5. Produce report comparing approaches of DSPT GAF-aligned and NCSC audits and develop recommendations on the best way to adopt an NCSC approach that's proportiionate and affordable.

Milestone/Deliverable	Deliverables/Tasks	Timeframe or Deliverv Date
Initiiation Meeting & Scoping	An initial meeting1between Buyer and Supplier to gain additional information and context regarding the Buyers organisation and to further clarify the scope.	Within week 1 of Contract Award
ReU1se the existing framework and repurpose for GAF keeping the same scoring outcomes	This activity will cover all Health and Care Organisations, as previously defined earlier in this document. The deliverable associated to this work is a stakeholder analysis that can be used to outline the scope of stakeholder engag1ement / interest in future activities.	Within 4 weeks
Test scoring outcomes using volunteer or faux audits	Test the scoring outcomes using 5 volunteer or faux audits	Within 3 weeks
Undertake post 910 live audits	Undertake post 910 live audits of 5 orqanisations	6 weeks post go live
Develop thematic report of the live audits	Thematic report of post go-live audits	within 8 weeks (to be undertaken in parallel with other tasks)
Comparative analysis of as-is and NCSG	Produce report comparing approaches with as-is and NCSG with recommendations on the best way to adopt an NCSC approach that's proportionate and affordable.	Within 4 weeks (can be initiated in parallel with other tasks)

7. Commissioning Process

Project specific statement of requirements for future call offs

7.1 Where the Buyer wishes *to* commission work under this Call Off Contract, it shall:

7.2 Detail the requirements for each individual project including millestones and acceptance criteria ("Project Requirements") substantially in the format set out in the Order Form.

7.3 The Buyer's commercial team will communicate Project Requirements to the Supplier whereupon the Supplier shall have five (5) worlking days (or an alternative period as set out by the Buyer upon communicating the Project Requirements) to respond. All commissioning requests shall be routed through the Commerciall department/dedicated Commercial Leads

7.4 The Supplier shall respond to the Project Requirements {the "Supplier's Solution"} in the format specified by the Buyer at the point of communicating the project requirements.

7.5 The Supplier's Solution shall include details of how the work will be undertaken, a timeline/activity plan along with CV's (if requested) and a summary of the expertise in the proposed resouircing model, it shall also include a detailed price for the delivery of the Project Requirements in the format provided by the Buyer. Where no format is specified, the method used to calculate the price shall be set out in sufficient detail for the Buyer to understand how the price was determined and, as a minimum, the Supplier's pricing will be broken down by the day rates of resources operating on each project and will be no more expensive than the day rates set out in its Tender..

7.6 In most instances, fixed fee or output-based pricing will be used. In other instances, capped T&M will be utilised based on the submitted rate card. The final decision would lie with the Buyer. Within five (5) workingidays of receiipt of the Supplier's Solution, or in any other period the Buyer deems appropriate, it shall review and feedback comments on the Supplier's Solution. Within two (2) working days of the Buyer providing this feedback (or an alternative period as set out by the Buyer upon communicating its feedback) the Supplier shall provide a final Supplier's Solution to the Buyer.

7. 7 Where the Buyer agrees with the Supplier's Solutiion the Buyer shall sign and return the Supplier's Solution to the Supplier for countersigning whereupon the Supplier shall commence delivery of the Services detailed in the Project Requirements and Supplier's Solution at the time agreed in the Project Requirements via the Buyer's online portal

7.8 Amendments to Project Requirements (and associated pricing) after the execution of the associated Project Requirements shall follow the

Variation process set out in Joint Schedule 2 of the Call-Off Contract and actioned through the Commercial Team

7.9 Close off from projects after the execution of a SOW shall be confirmed and signed off with the progrnmme.

7.10 At any point during or before the Commissioning Process, the Buyer may seelk alternative means of delivering the requirement includiing potentiallly recompeting the requirement.

7.11 The Call-Off Contract is non-exclusive, and the Buyer does not commit to awarding any work as part of this Call-Off Contract.

8. Manag,ement informatiion/reportiing

8. .1 The provider shall provide a monthly report to the Buyer to include the following information:

- Work package Commencement Date
- Work package Expiry Date
- Original vallue
- PO Number
- Invoices Paid to Date
- Outstanding invoices
- Balance
- Deliverables in the SOW
- Original work package Date, Revised Forecast Date
- Status - Not started, On-hold, In Progress, Completed, Cancelled, Variation (not in original work package)
- Satisfactorily meeting contract deliverables/KPls - Signoff (Yes/No)
- For Outcomes - Original Cost Per Deliverable, Forecast/ Actual Cost Per Deliverable
- For T&M - Role ID, Role, Original budget days, Forecast/ Actual days, Start Date, Planned End Date, Actual / Forecast End Date

8..2 If applicable to a specific SOW, a list of alll sub-contractors (inclluding Personal Service Companies)

8. .3 Supplier RAG - Supplier overall view **of** work package status

8.4 The supplier shall produce a weeklly progress report and update the NHSE Programme team at their weekly status meetiing.

8..5 All requests for information and responses to that information shall be stored on NHS England's central database.

9. Continuous improvement

9.1 The Buyer expects the supplier to continually improve the delivered services throughout the contract duration..

9.2 The supplier should present new ways of working to the Buyer during monthly/quarterly contract review meetings.

9.3 Changes to service delivery must be brought to the Buyer's attention and agreed upon before implementation.

10. Quality

10.1 The supplier's approach to the quality assurance process to ensure that the deliverables a.re of a high standard meet the releva.nt standards and other quality standaJds detailed in the high-level requirements document.

10.2 The Supplier must only deliver their work package using Cyber speciallist(s} with security clearance (Securiity Check (SC) clearance).

10.3 The Provider must be Cyber Essential plus and ISO 27001 compliant

11. Price

11.1 Prices are to be submitted viia the e-Sourcing Suite Atamis as an uploaded Price Schedule Template (in the Commercial Envelope) excluding VAT and including all other expenses relating to Contract delivery.

11.2 The provider will provide a costing model that reflects the SFIA day rate or industry standard equivalent of the cyber professionals to deliver each of the SOW's deliiverables with the flexibility to carry out further work as the Cyber Improvement progiramme progresses and discussion on priority areas of each workstream matures.

11.3 The applicable charging method(s) for this contract willl be based on fixed pricing with deliverables iissued through statement of works. The suppliers willll be required to provide day rate cards within the agreed maxiimum day rates for transparency.

11.4 No expenses other than approved travel in accordance with the NHSE Expense Policy shall be chargeable under this work package.

11.5 The provider will keep accurate records of the time spent by the Supplier staff in providing the services and will provide records to the Buyer for inspection on request.

11.6 The provider will keep an ongoiing record of spend to date, forecast spend to end of work package (by PO if the PO value differs}, and any forecast variation

of under or overspend ag1ainst each work package. The Supplier will provide records to the Buyer for iinspection on request.

12.. Staff and Buyer Service

12.1. he supplier shall ensure that staff understand the vision and objectives and provide excellent Buyer service to the Buyer throughout the duration of the Contract.

12.2. The supplier's staff assigned to the Contract shall have an excellent understanding of:

- The cyber threat landscape: the consultant should hold relevant compliance, technical or commercial roles.
- Industry-standard seourity architecture methodologies, frameworks, and best practices.
- The NHS and the health and care system.

12.3. The supplier shall provide their proposed project team, including a skills profile, and any knowledge-based specialities of relevant team members for each Call *Off* commissioned under this Call *Off* Contract

13. Security and confidentiality requirem,ents

13.1 he Provider must be compliant with alll the mandatory requirements detailed in the SQ- High Level Requirements..

13.2 The supplier's staff assigned to deliver the work package deliverables must have security check (SC) dearance.

13.3 The outputs of the statement of requirements and/or the results of the deliverables of the contract may involve working with classified material within our critical national infrastructure hence confidentiality/security restrictions will apply.

13.4 The supplier must have a good understanding of the Data Protectiion Legiislation, particularly the UK GDPR and Data Protection Act 2018 (DPA)..

14. Payment and invoicing

14.1 Payment - 30 days from the invoice date.

14.2. Invoices should be submitted via electronic invoicingiTradeshift. To register for Tradeshift please visit

https://nhssbs.support.tradeshift.com/ and view the section called 'Getting1 Started with Tradeshift'; or in the limited circumstances where electronic invoicing is not possible, please email invoices and credit notes to the folllowing email address sbs.apinvoicing@nhs.net with the billing1address on the invoice being:

NHS ENGLAND
X24 PAYABLES KOOS
K0OSPO BOX 312
LEEDS
LS11 1HP

14.3 Before payment can be considered, each invoice must include a detailed elemental breakdown of worikcompleted and the associated costs completed. Invoices should contain the folllowiing information.

- the purchase order number
- Appropriate reference and subject title of the SoW
- A copy of the deliverables/sign off criteria signed from the Programme Head/Lead.
- Expenses shall be suibject to NHSE expense policy.

Managing Public Money- Principles

14.4 NHS England have the responsibility to exercise proper stewardship of public funds, including compliance with the principles laid out in Managing Public Money. The standards ensure we are responsible for establishing and maintaining internal audit arrangements in accordance wiith the Public Sector Internal Audit Standards and have effective quality internal governance and sound financial management that demonstrates value for money.

14.5 All SOWs/work packages will be Fixed Priced or capped Time & Materials where payment will be made upon either:

- achievement of individual Milestones as detaiiled iin each SOW and/or Project Plans; or
- achievement of all Millestones detailed in the Project Requirements.

14.6 Pricing will be determined based on the rate card submitted during the Call Off Procedure and utillising the iincorporated discount mechanism submitted during that same procedure.

14.7 Payments cannot be verified without the supporting evidence.

14.8 Expenses shalll be subject to NHS **E** expense policy.

15. Contract manag,ement

15.1 The Progrnmme willl host an initiation meeting with relevant parties from the supplier organisation to commence the project.

15.2 We,ekly SOW review - weekly or as and when basiis

15.3 Monthly contractual! perfomiance - Reviiew Work Order periormance and feedback on meeting contract needs, Strategic discussions e.g..pipelline.

15.4 Quarterly contract reviews

15.5 Attendance at contract review meetings shall be a.t the suppliier's own expense.

16. Social value

16.1 Social value considerations form Pa.rt of the Technical Response Envelope and will be included in the Order Contract.

17. Locatiion

17.1 The location of the Services will be carried out remotely or at a UK based location, these are to be confirmed at each Call Off commiissioned..

Crown Commercial Service

Core Terms - DPS

1. Definitions used in the contract

1.1 Interpret this Contract using Joint Schedule 1 (Definitions).

2. How the contract works

2.1 The Supplier is eligible for the award of Order Contracts during the DPS Contract Period.

2.2 CCS doesn't guarantee the Supplier any exclusivity, quantity or value of work under the DPS Contract.

2.3 CCS has paid one penny to the Supplier legally to form the DPS Contract. The Supplier acknowledges this payment.

2.4 If the Buyer decides to buy Deliverables under the DPS Contract it must use DPS Schedule 7 (Order Procedure) and must state its requirements using DPS Schedule 6 (Order Form Template and Order Schedules). If allowed by the Regulations, the Buyer can:

- make changes to DPS Schedule 6 (Order Form Template and Order Schedules)
- create new Order Schedules
- exclude optional template Order Schedules
- use Special Terms in the Order Form to add or change terms

2.5 Each Order Contract:

- is a separate Contract from the DPS Contract
- is between a Supplier and a Buyer
- includes Core Terms, Schedules and any other changes or items in the completed Order Form
- survives the termination of the DPS Contract

2.6 Where the Supplier is approached by an eligible buyer requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this DPS Contract before accepting their order. The Supplier will promptly notify CCS if the eligible buyer won't use this DPS Contract.

2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.

2.8 The Supplier won't be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:

- verify the accuracy of the Due Diligence Information
- properly perform its own adequate checks

2.9 CCS and the Buyer won't be liable for errors, omissions or misrepresentation of any information.

2.10 The Supplier warrants and represents that all statements made and documents submitted as part of

the procurement of Deliverables are and remain true and accurate.

2.11 An Order Contract can only be created using the electronic procedures described in the OJEU Notice as required by the Regulations.

2.12 A Supplier can only receive Orders under the DPS Contract while it meets the basic access requirements for the DPS stated in the OJEU Notice. CCS can audit whether a Supplier meets the basic access requirements at any point during the DPS Contract Period.

3. What needs to be delivered

3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

- that comply with the Specification, the DPS Application and, in relation to an Order Contract, the Order Tender (if there is one)
- to a professional standard
- using reasonable skill and care
- using Good Industry Practice
- using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract
- on the dates agreed
- that comply with Law

3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.

3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.

3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.

3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with Clause 3. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

3.3 Services clauses

3.3.1 Late Delivery of the Services will be a Default of an Order Contract.

3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.

3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.

3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.

3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

4 Pricing and payments

4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.

4.2 CCS must invoice the Supplier for the Management Levy and the Supplier must pay it using the process in DPS Schedule 5 (Management Levy and Information).

4.3 All Charges and the Management Levy:

- exclude VAT, which is payable on provision of a valid VAT invoice
- include all costs connected with the Supply of Deliverables

4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.

4.5 A Supplier invoice is only valid if it:

- includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer
- includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any)
- doesn't include any Management Levy (the Supplier must not charge the Buyer in any way for the Management Levy)

4.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

4.7 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, CCS or the Buyer can publish the details of the late payment or non-payment.

4.8 If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables and that cost is reimbursable by the Buyer, then CCS or the Buyer may either:

- require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items
- enter into a direct agreement with the Subcontractor or third party for the relevant item

4.9 If CCS or the Buyer uses Clause 4.8 then the Charges must be reduced by an agreed amount by using the Variation Procedure.

4.10 CCS and the Buyer's right to enter into a direct agreement for the supply of the relevant items is subject to both:

- the relevant item being made available to the Supplier if required to provide the Deliverables
- any reduction in the Charges excluding any unavoidable costs that must be paid by the Supplier for the substituted item, including any licence fees or early termination charges

4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they're ordered to do

so by a court.

5. The buyer's obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

- neither CCS or the Buyer can terminate a Contract under Clause 10.4.1
- the Supplier is entitled to reasonable and proven additional expenses and to relief from Delay Payments, liability and Deduction under this Contract
- the Supplier is entitled to additional time needed to make the Delivery
- the Supplier cannot suspend the ongoing supply of Deliverables

5.2 Clause 5.1 only applies if the Supplier:

- gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware
- demonstrates that the Supplier Non-Performance only happened because of the Authority Cause
- mitigated the impact of the Authority Cause

6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the End Date.

6.3 The Supplier must allow any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit.

6.4 The Supplier must provide information to the Auditor and reasonable co-operation at their request.

6.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

- tell the Relevant Authority and give reasons
- propose corrective action
- provide a deadline for completing the corrective action

6.6 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:

- the methodology of the review
- the sampling techniques applied
- details of any issues

- any remedial action taken

6.7 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

7.1 The Supplier Staff involved in the performance of each Contract must:

- be appropriately trained and qualified
- be vetted using Good Industry Practice and the Security Policy
- comply with all conduct requirements when on the Buyer's Premises

7.2 Where a Buyer decides one of the Supplier's Staff isn't suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.

7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.

7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

8.1 The Supplier warrants and represents that:

- it has full capacity and authority to enter into and to perform each Contract
- each Contract is executed by its authorised representative
- it is a legally valid and existing organisation incorporated in the place it was formed
- there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract
- it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract
- it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract
- it is not impacted by an Insolvency Event
- it will comply with each Order Contract

8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.

8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:

- wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract
- non-payment by the Supplier of any tax or National Insurance

8.4 All claims indemnified under this Contract must use Clause 26.

8.5 CCS or a Buyer can terminate the Contract for breach of any warranty or indemnity where they are entitled to do so.

8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.

8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to both:

- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier

9.2 Any New IPR created under an Order Contract is owned by the Buyer. The Buyer gives the Supplier i) a licence to use any Buyer Existing IPRs and New IPR during the Order Contract Period for the purpose of fulfilling its obligations under the Order Contract, and ii) a licence to use the New IPRs (excluding any Information which is the Buyers Confidential information or which is subject to the Data Protection Legislation) after the Order Contract period on the terms set out in the Open Government Licence. "

9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:

- obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR

- replace or modify the relevant item with substitutes that don't infringe IPR without adversely affecting the functionality or performance of the Deliverables

10. Ending the contract

10.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

10.3 Ending the contract without a reason

10.3.1 CCS has the right to terminate the DPS Contract at any time without reason or liability by giving the Supplier at least 30 days' notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.3.2 Each Buyer has the right to terminate their Order Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- there's a Supplier Insolvency Event
- there's a Contract Default that is not corrected in line with an accepted Rectification Plan
- the Relevant Authority rejects a Rectification Plan or the Supplier does not provide it within 10 days of the request
- there's any material default of the Contract
- there's a Default of Clauses 2.10, 9, 14, 15, 27, 32 or DPS Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract
- there's a consistent repeated failure to meet the Performance Indicators in DPS Schedule 4 (DPS Management)
- there's a Change of Control of the Supplier which isn't pre-approved by the Relevant Authority in writing
- there's a Variation to a Contract which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes)
- if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded
- the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union (TFEU) to declare that the Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations
- the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them

10.4.2 CCS may terminate the DPS Contract if a Buyer terminates an Order Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If there is a Default, the Relevant Authority can, without limiting its other rights, request that the Supplier provide a Rectification Plan.

10.4.4 When the Relevant Authority receives a requested Rectification Plan it can either:

- reject the Rectification Plan or revised Rectification Plan, giving reasons
- accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties

10.4.5 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

- must give reasonable grounds for its decision
- may request that the Supplier provides a revised Rectification Plan within 5 Working Days

10.4.6 If any of the events in 73 (1) (a) to (c) of the Regulations happen, the Relevant Authority has the right to immediately terminate the Contract and Clause 10.5.2 to 10.5.7 applies.

10.5 What happens if the contract ends

Where the Relevant Authority terminates a Contract under Clause 10.4.1 all of the following apply:

10.5.1 The Supplier is responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.
10.5.2 The Buyer's payment obligations under the terminated Contract stop immediately.
10.5.3 Accumulated rights of the Parties are not affected.
10.5.4 The Supplier must promptly delete or return the Government Data except where required to retain copies by law.
10.5.5 The Supplier must promptly return any of CCS or the Buyer's property provided under the terminated Contract.
10.5.6 The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).
10.5.7 The following Clauses survive the termination of each Contract: 3.2.10, 6, 7.2, 9, 11, 14, 15, 16, 17, 18, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.6 When the supplier can end the contract

10.6.1 The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate an Order Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

10.6.2 If a Supplier terminates an Order Contract under Clause 10.6.1:

- the Buyer must promptly pay all outstanding Charges incurred to the Supplier
- the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the

Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated
- Clauses 10.5.4 to 10.5.7 apply

10.7 When subcontracts can be ended

At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:

- there is a Change of Control of a Subcontractor which isn't pre-approved by the Relevant Authority in writing
- the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4
- a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority

10.8 Partially ending and suspending the contract

10.8.1 Where CCS has the right to terminate the DPS Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Order Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Order Contracts that have already been signed.

10.8.2 Where CCS has the right to terminate a DPS Contract it is entitled to terminate all or part of it.

10.8.3 Where the Buyer has the right to terminate an Order Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

10.8.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

10.8.5 The Parties must agree any necessary Variation required by Clause 10.8 using the Variation Procedure, but the Supplier may not either:

- reject the Variation
- increase the Charges, except where the right to partial termination is under Clause 10.3

10.8.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.8.

11. How much you can be held responsible for

11.1 Each Party's total aggregate liability in each Contract Year under this DPS Contract (whether in tort, contract or otherwise) is no more than £100,000.

11.2 Each Party's total aggregate liability in each Contract Year under each Order Contract (whether in tort,

contract or otherwise) is no more than the greater of £1 million or 150% of the Estimated Yearly Charges unless specified in the Order Form

11.3 No Party is liable to the other for:

- any indirect Losses
- Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect)

11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

- its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors
- its liability for bribery or fraud or fraudulent misrepresentation by it or its employees
- any liability that cannot be excluded or limited by Law
- its obligation to pay the required Management Levy

11.5 In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3, 9.5, 12.2 or 14.8 or Order Schedule 2 (Staff Transfer) of a Contract.

11.6 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

11.7 When calculating the Supplier's liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

- Deductions
- any items specified in Clause 11.5

11.8 If more than one Supplier is party to a Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 The Supplier indemnifies CCS and every Buyer against any costs resulting from any Default by the Supplier relating to any applicable Law to do with a Contract.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance

Requirements) and any Additional Insurances in the Order Form.

14. Data protection

14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

- tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier
- restore the Government Data itself or using a third party

14.7 The Supplier must pay each Party's reasonable costs of complying with Clause 14.7 unless CCS or the Buyer is at fault.

14.8 The Supplier:

- must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request
- must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading
- must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice
- securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it
- Indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

14.9. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the

spread of, and minimise the impact of Malicious Software.

14.10 If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

14.11. Any cost arising out of the actions of the Parties taken in compliance with the provisions of Clause shall be borne by the Parties as follows:

14.11.1 by the Supplier, where the Malicious Software originates from the software provided by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Relevant Authority when provided to the Supplier; and

14.11.2. by the Relevant Authority, if the Malicious Software originates from the software provided by the Relevant Authority or the Government Data (whilst the Government Data was under the control of the Relevant Authority)."The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

15. What you must keep confidential

15.1 Each Party must:

- keep all Confidential Information it receives confidential and secure
- not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent, except for the purposes anticipated under the Contract
- immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

- where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure
- if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party
- if the information was given to it by a third party without obligation of confidentiality
- if the information was in the public domain at the time of the disclosure
- if the information was independently developed without access to the Disclosing Party's Confidential Information
- to its auditors or for the purposes of regulatory requirements
- on a confidential basis, to its professional advisers on a need-to-know basis
- to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

15.4 CCS or the Buyer may disclose Confidential Information in any of the following cases:

- on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer
- on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to
- if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions
- where requested by Parliament
- under Clauses 4.7 and 16

15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

15.6 Transparency Information is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

16.2 Within the required timescales the Supplier must give CCS and each Buyer full co-operation and information needed so the Buyer can:

- publish the Transparency Information
- comply with any Freedom of Information Act (FOIA) request
- comply with any Environmental Information Regulations (EIR) request

16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority's decision, which does not need to be reasonable.

17. Invalid parts of the contract

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it's valid or enforceable.

18. No other terms apply

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

19. Other people's rights in a contract

No third parties may use the Contracts (Rights of Third Parties) Act (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

- provides a Force Majeure Notice to the other Party
- uses all reasonable measures practical to reduce the impact of the Force Majeure Event

20.2 Either party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

20.3 Where a Party terminates under Clause 20.2:

- each party must cover its own Losses
- Clause 10.5.2 to 10.5.7 applies

21. Relationships created by the contract

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 The Supplier can not assign a Contract without the Relevant Authority's written consent.

23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Relevant Authority.

23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.

23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

- their name
- the scope of their appointment
- the duration of their appointment

24. Changing the contract

24.1 Either Party can request a Variation to a Contract which is only effective if agreed in writing and signed by both Parties.

24.2 The Supplier must provide an Impact Assessment either:

- with the Variation Form, where the Supplier requests the Variation
- within the time limits included in a Variation Form requested by CCS or the Buyer

24.3 If the Variation to a Contract cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

- agree that the Contract continues without the Variation
- terminate the affected Contract, unless in the case of an Order Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them
- refer the Dispute to be resolved using Clause 34 (Resolving Disputes)

24.4 CCS and the Buyer are not required to accept a Variation request made by the Supplier.

24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the DPS Pricing or the Charges.

24.6 If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, DPS Pricing or a Contract and provide evidence:

- that the Supplier has kept costs as low as possible, including in Subcontractor costs
- of how it has affected the Supplier’s costs

24.7 Any change in the DPS Pricing or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

25. How to communicate about the contract

25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

25.2 Notices to CCS must be sent to the CCS Authorised Representative's address or email address indicated on the Platform.

25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Order Form.

25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

26.2 At the Indemnifier's cost the Beneficiary must both:

- allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim
- give the Indemnifier reasonable assistance with the claim if requested

26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.

26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that doesn't damage the Beneficiary's reputation.

26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

- the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money
- the amount the Indemnifier paid the Beneficiary for the Claim

27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Contract Period:

- commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2)
- do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them

27.2 The Supplier must during the Contract Period:

- create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same
- keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request
- if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses 27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

- been investigated or prosecuted for an alleged Prohibited Act
- been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency
- received a request or demand for any undue financial or other advantage of any kind related to a Contract
- suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act

27.4 If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.4 it must specify the:

- Prohibited Act
- identity of the Party who it thinks has committed the Prohibited Act
- action it has decided to take

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the

Contract, including:

- protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise
- any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

- all applicable Law regarding health and safety
- the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer Premises that relate to the performance of a Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

31. Tax

31.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

- the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant
- other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may reasonably need

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance

contributions in the UK relating to payment received under an Order Contract, the Supplier must both:

- comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions
- indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

- the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding
- the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer
- the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements
- the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

- Law
- Clause 12.1
- Clauses 27 to 32

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach

listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

- determine the Dispute
- grant interim remedies
- grant any other provisional or protective relief

34.4 The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

34.5 The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

34.6 The Supplier cannot suspend the performance of a Contract during any Dispute.

35. Which law applies

This Contract and any issues arising out of, or connected to it, are governed by English law.

36. Buyer Premises

36.1 Licence to occupy Buyer Premises

36.1.1. Any Buyer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this Order Contract. The Supplier shall have the use of such Buyer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Order Contract.

36.1.2. The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Order Contract and the Supplier shall co-operate (and ensure that

the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.

36.1.3. Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of Order Schedule 6 (where used) and set out in the Order Form (or elsewhere in the relevant Order Contract), should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any modification work which it approves pursuant to this Clause 36.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

36.1.4. The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.

36.1.5. The Parties agree that there is no intention on the part of the Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to the relevant Order Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

36.2 Security of Buyer Premises

36.2.1 The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.

36.2.2 The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

37. Buyer Property

37.1 Where the Buyer issues Buyer Property free of charge to the Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.

37.2 The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.

37.3 The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.

37.4 The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.

37.5 The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with the relevant Order Contract and for no other purpose without Approval.

37.6 The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance Order Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.

37.7 The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and

tear), unless such loss or damage was solely caused by a Buyer Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

38. Buyer Equipment

38.1 Unless otherwise stated in the relevant Order Contract, the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

38.2 The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

38.3 The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Contract Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

38.4 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

38.5 Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Order Contract, including the Service Levels.

38.6 The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

38.7 The Supplier shall, at the Buyer's written request, at its own expense and as soon as reasonably practicable:

38.7.1 Remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with the Order Contract; and

38.7.2 Replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.