

Order Form

CALL-OFF REFERENCE: BSP_6115 / ITT_4672. Contract Ref: C048707

Public Heath England: Public Heath Infectious Disease Case and Incident Management System

THE BUYER: The Secretary of State for Health and Social Care acting as part of the Crown through Public Health England

BUYER ADDRESS Wellington House 133-155 Waterloo Road
London, SE1 8UG

THE SUPPLIER: Insight Direct (UK) Ltd

SUPPLIER ADDRESS: The Technology Building, Insight Campus, Terry Street, Sheffield, S9 2BU

REGISTRATION NUMBER: 2579852

DUNS NUMBER: 76-938-7739

SID4GOV ID: 208171

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 27 September 2021.

It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

Following a change to public health organisational structures, Public Health England (PHE) is to be phased out on the 30th September 2021. A new body, the United Kingdom Health Security Agency (UKHSA) will be the Buyer responsible for this Call-Off Contract from 1st October 2021. From this date forwards, any reference to Public Health England (PHE) will be replaced by the United Kingdom Health Security Agency (UKHSA) in this Call-Off Contract and all its documents.

CALL-OFF LOT(S):

- Lot 3 Software & Associated Services

CALL-OFF INCORPORATED TERMS

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

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6068
3. Annexes D to Call-Off Schedule 6 (ICT Services)
4. The following Schedules in equal order of precedence:
 - *Joint Schedules for RM6068*
 - *Joint Schedule 2 (Variation Form)*
 - *Joint Schedule 3 (Insurance Requirements)*
 - *Joint Schedule 4 (Commercially Sensitive Information)*
 - Joint Schedule 6 (Key Subcontractors)
 - *Joint Schedule 10 (Rectification Plan)*
 - *Joint Schedule 11 (Processing Data)*
 - *Call-Off Schedules for*
 - Call-Off Schedule 5 (Pricing Details)
 - Call-Off Schedule 6 (ICT Services)
 - Call-Off Schedule 7 (Key Supplier Staff)
 - Call-Off Schedule 8 (Business Continuity & Disaster Recovery *Part B*)
 - Call-Off Schedule 9 (Security) *Part B*
 - Call-Off Schedule 10 (Exit Management) *Part A*
 - Call-Off Schedule 13 (Implementation Plan and Testing)
 - Call-Off Schedule 14 (Service Levels)
 - Call-Off Schedule 20 (Call-Off Specification)
5. CCS Core Terms (version 3.0.6)
6. Joint Schedule 5 (Corporate Social Responsibility) RM6068
7. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off 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 Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

None

CALL-OFF START DATE: 30 September 2021

CALL-OFF EXPIRY DATE: 29 September 2026

CALL-OFF INITIAL PERIOD: Five (5) Years

CALL-OFF OPTIONAL EXTENSION None

CALL-OFF DELIVERABLES

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

LOCATION FOR DELIVERY

Work may be done remotely. The service will be used in PHE locations around the UK and Northern Ireland. Attendance at offices across the UK may be required, within COVID-19 restrictions, after a risk assessment has been undertaken and subject to current guidance and legislation.

DATES FOR DELIVERY OF THE DELIVERABLES

Option A: Delivery date details the agreed:

- The agreed SaaS configured for PHE infectious disease management requirements including the management of the COVID disease within eight (8) Weeks of the Call Off Start Date (Please refer to Annex 4 COVID Process Form); and
- the managed service is to be delivered during the course of the Call-Off Period,
as further detailed in the Call-Off Schedule 20.

TESTING OF DELIVERABLES

See details in Call-Off Schedule 13 (Implementation Plan & Testing)

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be a minimum of 90 (ninety) days.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £4,038,065.05 (four million and thirty-eight thousand pounds).

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details) - total call-off charges over the initial period are £9,384,183.46.

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

Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

See details in Call-Off Schedule 5 (Pricing Details)

PAYMENT METHOD

BACS on receipt of a valid invoice that must contain a valid PHE (Purchase Order PO number.

BUYER'S INVOICE ADDRESS*:

Accounts Payable
Public Health England
PHE Porton Down
Manor Farm Road
Salisbury
Wiltshire
SP4 0JG

**Invoices must be emailed to the following address Payables@phe.gov.uk as paper copies are not being accepted at this time owing to COVID-19.*

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]
Deputy Head Procurement

[REDACTED]
Public Health England
Wellington House
133-155 Waterloo Road
London, SE1 8UG

BUYER'S ENVIRONMENTAL POLICY

PHE Environmental Policy.pdf

BUYER'S SECURITY POLICY

PHE Security Principles.pdf

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]
Public Sector Business Development Director

[REDACTED]
5th Floor, Metro Building
Trafford Road
Salford Quays
Manchester

M5 3NN

SUPPLIER'S CONTRACT MANAGER



PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month and project updates as stated in the Tender and agreed from time to time.

PROGRESS MEETING FREQUENCY

Quarterly on the first Working Day of each quarter and project meetings as stated in the Tender and agreed from time to time.

KEY STAFF

As set out in Call Off Schedule 7 – Key Supplier Staff

KEY SUBCONTRACTOR(S)

Conduent Public Health Solutions, Inc

COMMERCIALLY SENSITIVE INFORMATION

Call-Off Schedule 5

SERVICE CREDITS

In accordance with Schedule 14 where the Service Period means one Month. Service Levels and Service Credits do not apply during Implementation, however these will apply during the pilot phase and subsequent Deliverables, as defined in the Implementation Plan.

ADDITIONAL INSURANCES


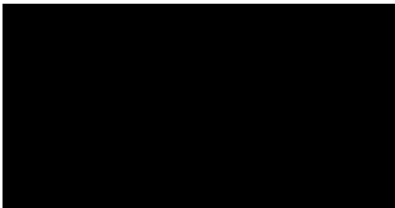
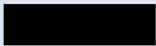
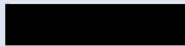
Not applicable.

GUARANTEE

Not Applicable.

SOCIAL VALUE COMMITMENT

Shall be as stated in the Supplier's Tender.

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:		Signature:	
Name:		Name:	
Role:	Public Sector Business Development Director	Role:	Interim Chief Executive, PHE
Date:	23 September 2021	Date:	27 September 2021

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 it 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:

"Additional Insurances"	insurance requirements relating to a Call-Off 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;
"Associated Services"	the Associated Services detailed in Framework Schedule 1 and available for Buyers to procure as part of a Call-Off Contract that also involves the supply of Goods;
"Audit"	<p>the Relevant Authority's right to:</p> <ul style="list-style-type: none"> a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off 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,

	<p>ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;</p> <p>h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;</p> <p>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;</p> <p>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; or</p> <p>k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;</p>
"Auditor"	<p>a) the Relevant Authority's internal and external auditors;</p> <p>b) the Relevant Authority's statutory or regulatory auditors;</p> <p>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;</p> <p>d) HM Treasury or the Cabinet Office;</p> <p>e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and</p> <p>f) successors or assigns of any of the above;</p>
"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 Call-Off 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);
"Call-Off Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
"Call-Off Contract Period"	the Contract Period in respect of the Call-Off Contract;
"Call-Off Expiry Date"	the date of the end of a Call-Off Contract as stated in the Order Form;
"Call-Off Incorporated Terms"	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
"Call-Off Initial Period"	the Initial Period of a Call-Off Contract specified in the Order Form;
"Call-Off Optional Extension Period"	such period or periods beyond which the Call-Off Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form;
"Call-Off Procedure"	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Procedure and Award Criteria);
"Call-Off Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract;
"Call-Off Start Date"	the date of start of a Call-Off Contract as stated in the Order Form;
"Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender) where this is used;
"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 Framework Contract initially identified in the Framework Award Form;

"Central Government Body"	<p>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:</p> <p>a) Government Department;</p> <p>b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);</p> <p>c) Non-Ministerial Department; or</p> <p>d) Executive Agency;</p>
"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 Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off 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 Framework Award 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;
"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
"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 Framework Contract or the Call-Off Contract, as the context requires;
"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"Contract Period"	the term of either a Framework Contract or Call-Off 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 Framework Contracts and Call-Off 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;

	<p>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;</p> <p>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; and</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;</p> <p>but excluding:</p> <p>a) Overhead;</p> <p>b) financing or similar costs;</p> <p>c) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise;</p> <p>d) taxation;</p> <p>e) fines and penalties;</p> <p>f) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and</p> <p>g) non-cash items (including depreciation, amortisation, impairments and movements in provisions);</p>
"Crown Body"	<p>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;</p>
"CRTPA"	<p>the Contract Rights of Third Parties Act 1999;</p>
"Data Loss Event"	<p>any event that results, or may result, in unauthorised access to Personal Data held by the Supplier 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;</p>

"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 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;
"Dead on Arrival/Installation" or "DOA" or "DOI"	means once removed from its packaging at a Buyer's premises, the delivered device fails to work in accordance with the manufacturer's specification;
"Deductions"	all Service Credits, Delay Payments (in both cases if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off 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 Charge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges 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 a Call-Off Contract as confirmed and accepted by the Buyer in writing to the Supplier. "Deliver" and "Delivered" shall be construed accordingly;
"Device as a Service"	a sourcing model whereby the Buyer pays a subscription for the provision by the Supplier of a hardware device together with bundled software and/or services

"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"	<p>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:</p> <p>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</p> <p>b) is required by the Supplier in order to provide the Deliverables; and/or</p> <p>c) has been or shall be generated for the purpose of providing the Deliverables;</p>
"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;
"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;
"Endemic Failure"	means a failure rate equal to or above 300% the mean time to failure under Goods testing by the manufacturer
"End of Life (EOL)"	means the Goods are no longer being manufactured and there is insufficient stock of such Goods available in the supply chain to meet the full Buyer requirement and/or Order.
"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 Charges"	the anticipated total Charges payable by the Buyer 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 Charges; or ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off 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 Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);

"Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;
"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"	<p>any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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;
"Framework Award Form"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
"Framework Contract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;
"Framework Contract Period"	the period from the Framework Start Date until the End Date or earlier termination of the Framework Contract;
"Framework Expiry Date"	the date of the end of the Framework Contract as stated in the Framework Award Form;
"Framework Incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;

"Framework Initial Period"	the initial term of the Framework Contract as specified in the Framework Award Form;
"Framework Optional Extension Period"	such period or periods beyond which the Framework Initial Period may be extended up to a maximum of the number of years in total specified in the Framework Award Form;
"Framework Price(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
"Framework Special Terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
"Framework Start Date"	the date of start of the Framework Contract as stated in the Framework Award Form;
"Framework Tender Response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender Response);
"Further Competition Procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Procedure and Award Criteria);
"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; 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 Framework Schedule 1 (Specification) and in relation to a Call-Off 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:

	<p>i) are supplied to the Supplier by or on behalf of the Authority; or</p> <p>ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract; or</p> <p>b) any Personal Data for which the Authority is the Data Controller;</p>
"Government Procurement Card"	<p>the Government's preferred method of purchasing and payment for low value goods or services;</p> <p>https://www.gov.uk/government/publications/government-procurement-card--2;</p>
"Guarantor"	<p>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;</p>
"Halifax Abuse Principle"	<p>the principle explained in the CJEU Case C-255/02 Halifax and others;</p>
"HMRC"	<p>Her Majesty's Revenue and Customs;</p>
"ICT Policy"	<p>the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;</p>
"Impact Assessment"	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <p>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;</p> <p>b) details of the cost of implementing the proposed Variation;</p> <p>c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/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;</p> <p>d) a timetable for the implementation, together with any proposals for the testing of the Variation; and</p> <p>e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;</p>
"Implementation Plan"	<p>the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;</p>
"Indemnifier"	<p>a Party from whom an indemnity is sought under this Contract;</p>
"Information"	<p>has the meaning given under section 84 of the Freedom of Information Act 2000;</p>
"Information assurance (IA)"	<p>is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes</p>

"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 in the Framework Award Form or the Order Form, as the context requires;
"Insolvency Event"	<p>a) in respect of a person:</p> <p>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</p> <p>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</p> <p>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</p> <p>e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or</p> <p>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</p> <p>g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or</p> <p>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</p> <p>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</p> <p>j) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;</p>
"Installation Works"	all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract;
"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;

	<p>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</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction;</p>
"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"	<p>any Subcontractor:</p> <p>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</p> <p>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</p> <p>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 Call-Off Contract,</p> <p>and the Supplier shall list all such Key Subcontractors in section 20 of the Framework Award Form and in the Key Subcontractor Section in Order Form;</p>
"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 Supplier 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;
"Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
"Man Day"	7.5 Man Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
"Management Charge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
"Management Information" or "MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);
"Margin"	means the percentage by which the price for Goods exceeds the Supplier's costs in relation to those Goods, excluding any other supply chain rebates and shipping/delivery
"Marketing Contact"	shall be the person identified in the Framework Award 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 Framework Schedule 5 (Management Charges and Information);
"MI Reporting Template"	means the form of report set out in the Annex to Framework Schedule 5 (Management Charges 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;
"Milestone Payment"	a payment identified in the Implementation Plan to be made following the satisfactory achievement of the relevant Milestone;

"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"	<p>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</p> <p>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;</p> <p>but shall not include the Supplier's Existing IPR;</p>
"Occasion of Tax Non-Compliance"	<p>where:</p> <p>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:</p> <ul style="list-style-type: none"> 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 <p>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;</p>
"Open Book Data"	<p>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 Call-Off Contract, including details and all assumptions relating to:</p> <p>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;</p> <p>b) operating expenditure relating to the provision of the Deliverables including an analysis showing:</p> <ul style="list-style-type: none"> 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)

	<p>together with a list of agreed rates against each manpower grade;</p> <p>iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and</p> <p>iv) Reimbursable Expenses, if allowed under the Order Form;</p> <p>c) Overheads;</p> <p>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;</p> <p>e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis;</p> <p>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;</p> <p>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</p> <p>h) the actual Costs profile for each Service Period;</p>
"Open Source"	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;
"Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
"Order Form Template"	the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules);
"Other Contracting Authority"	any actual or potential Buyer under the Framework 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 Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off 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 Framework Contract set out in Framework Schedule 4 (Framework 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;
"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. "Process" and "Processed" shall be interpreted accordingly;
"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"	<p>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:</p> <ul style="list-style-type: none"> 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; <p>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</p> <p>c) committing any offence:</p>

	<ul style="list-style-type: none"> 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"	<p>technical and organisational measures which must take account of:</p> <ul style="list-style-type: none"> a) the nature of the data to be protected b) harm that might result from Data Loss Event; c) state of technological development d) the cost of implementing any measures <p>including but not limited to 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;</p>
"Public Services Network or PSN"	<p>the network of networks delivered through multiple service providers, as further detailed in the PSN operating model; and described at https://www.gov.uk/government/groups/public-servicesnetwork;</p>
"Purchase to Pay" or "P2P"	<p>means an electronic system used to host a catalogue that allows for the full procurement process, from ordering through to invoice. The "official" definition of Purchase to Pay according to the Chartered Institute of Purchasing and Supply: "A seamless process enabled by technology designed to speed up the process from point of order to payment." For more information on MOD's P2P system see: www.d2btrade.com;</p>
"Recall"	<p>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 IPR rights) that might endanger health or hinder performance;</p>
"Recipient Party"	<p>the Party which receives or obtains directly or indirectly Confidential Information;</p>
"Rectification Plan"	<p>the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan Template) which shall include:</p> <ul style="list-style-type: none"> 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"	<p>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:</p> <p>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</p> <p>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;</p>
"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"	<p>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);</p> <p>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</p> <p>information derived from any of the above;</p>
"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 Call-Off 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 Framework Contract or Call-Off Contract which contains important information specific to each aspect of buying and selling;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off 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 Framework 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 Call Off Contract (which, where Call Off 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 Framework Schedule 1 (Specification) and in relation to a Call-Off 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;
"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;
"Software as a Service (SaaS)"	a software solution that involves the Buyer using applications sourced via the Supplier and running on a cloud infrastructure which is not managed or controlled by the Buyer. The applications are accessed from client devices through a thin client interface such as a web browser or a program interface
"Special Terms"	any additional Clauses set out in the Framework Award 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 Framework Schedule 1 (Specification), as may, in relation to a Call-Off 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 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 Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off 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 Call-Off 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 a Call-Off Contract or the Framework 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 the Processor related to a Contract;
"Supplier"	the person, firm or company identified in the Framework Award Form or Order Form as appropriate;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off 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 Call-Off 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 Call-Off Contract;
"Supplier Framework Manager"	a suitably qualified contact nominated by the Supplier who will take overall responsibility for delivering the Goods and/or Services required within the Framework Contract.
"Supplier Non-Performance"	where the Supplier has failed to:

	<p>a) Achieve a Milestone by its Milestone Date;</p> <p>b) provide the Goods and/or Services in accordance with the Service Levels ; and/or</p> <p>c) comply with an obligation under a Contract;</p>
"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 a Call-Off 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 Review Meeting"	a performance review meeting to take regularly place throughout the Framework Contract Period at which the Parties will review the Supplier's performance under the Framework Contract
"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 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 Call-Off 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 Call-Off Contract as set out in a) the Order Form, or b) the Test Plan agreed pursuant to Part B of Call-Off Schedule 13, and "Testing" and "Tested" shall be construed accordingly;
"Test Device"	means a device provided by the Supplier to the Buyer for the purposes of testing compatibility of the Goods with the Buyer's IT infrastructure. The Test Device shall be an exact sample of the Goods specified in the Order Form;
"Test Period"	the period specified in a) the Order Form, or b) Part A to Call-Off Schedule 13 during which Testing shall be carried out.
"Test Success Criteria"	the criteria specified in a) the Order Form, or b) the Test Plan agreed pursuant to Part B of Call-Off Schedule 13 that the relevant Deliverables must satisfy for the relevant Test to be recorded as successful.
"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 Call-Off Schedule 1 (Transparency Reports);
"US-EU Privacy Shield Register"	a list of companies maintained by the United States of America Department for Commerce 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:	Buyer ("the Buyer") And Insight Direct (UK) Ltd ("the Supplier")	
Contract name:	Public Heath England: Public Heath Infectious Disease Case and Incident Management System ("the Contract")	
Contract reference number:	BSP_6115 ITT_4672	
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: <ul style="list-style-type: none"> [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 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.

Order Form & Schedules
Public Heath England: Public Heath Infectious Disease Case and Incident Management System

Signed by an authorised signatory for and on behalf of the Buyer

Signature

Date

Name (in Capitals)

Address

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

Signature

Date

Name (in Capitals)

Address

Joint Schedule 3 (Insurance Requirements)

2. The insurance you need to have

- 2.1 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 a Call-Off 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:
 - 2.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 2.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 2.2 The Insurances shall be:
 - 2.2.1 maintained in accordance with Good Industry Practice;
 - 2.2.2 (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;
 - 2.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 2.2.4 maintained for at least six (6) years after the End Date.
- 2.3 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.

3. How to manage the insurance

- 3.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 3.1.1 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;
 - 3.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 3.1.3 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.

4. What happens if you aren't insured

- 4.1 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.
- 4.2 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.

5. Evidence of insurance you must provide

- 5.1 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.

6. Making sure you are insured to the required amount

- 6.1 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.

7. Cancelled Insurance

- 7.1 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.
- 7.2 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.

8. Insurance claims

- 8.1 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.

- 8.2 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.
- 8.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 8.4 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.

Joint Schedule 4 (Commercially Sensitive Information)

9. What is the Commercially Sensitive Information?

- 9.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 9.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 9.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	Contract Signature Date	Call Off Schedule 20 – Call Off Tender	Contract duration plus 24 months
2	Contract Signature Date	Call Off Schedule 5 – Pricing	Contract duration plus 24 months
3	Contract Signature Date	Call Off Schedule 13 – Implementation Plan and Testing	Contract duration plus 24 months

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the Framework 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) – all Lots;
 - 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 one million pounds (£1,000,000) – all Lots;
 - 1.3 employers' 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) – all Lots; and
 - 1.4 product liability 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) – all Lots.

Call-Off Schedule 4 (Call Off Tender)



PHE ID_CIMS Further
Comp_RM6068 (TePA



Annex 3 - System
Map.pdf



Annex 2 - PHE
Security Principles.pdf
environmental_policy.



PHE
environmental_policy.



Annex 7 - CIMS
Sample Data.csv



Annex 6 - CIMS
Combined ITT Process Scenarios for Demos,



Annex 5 - CIMS
Combined ITT Process Scenarios for Demos,



Annex 4 - Health and
Social Care Cloud Sec

Call-Off Schedule 5 (Pricing Details)

Pricing is as summarised below

	Year 1	Year 2	Year 3	Year 4	Year 5	Total
	GDP	GDP	GDP	GDP	GDP	
Build						
Ongoing Hosting, Maintenance and Support						
Total						£9,384,183.46

And set out in further detail in

- Price Template Submission
- P1 Insight and Conduent Infectious Disease CIMS_ITT4672_Pricing Template v2; and
- P2 Addendum to CIMS Pricing-Assumptions.
- Payment Milestone Schedule to be included in the final Implementation Plan

Call-Off 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):

- | | |
|-----------------------------|--|
| 1.5 "Buyer Property" | 1.6 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 Contract; |
| 1.7 "Buyer Software" | 1.8 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; |
| 1.9 "Buyer System" | 1.10 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 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; |
| 1.11 "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 |
| 1.12 | 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 Call Off 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 Contract;

1.13	"Emergency Maintenance"	1.14	ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;
1.15	"ICT Environment"	1.16	the Buyer System and the Supplier System;
1.17	"Licensed Software"	1.18	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 Call Off Contract, including any COTS Software;
1.19	"Maintenance Schedule"	1.20	has the meaning given to it in paragraph 8 of this Schedule;
1.21	"Malicious Software"	1.22	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;
1.23	"New Release"	1.24	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;
1.25	"Open Source Software"	1.26	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;
1.27	"Operating Environment"	1.28	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:

- e) the Deliverables are (or are to be) provided;
or
- f) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or
- g) where any part of the Supplier System is situated;

1.29	"Permitted Maintenance"	1.30	has the meaning given to it in paragraph 8.2 of this Schedule;
1.31	"Quality Plans"	1.32	has the meaning given to it in paragraph 6.1 of this Schedule;
1.33	"Sites"	1.34	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
1.35	"Software"	1.36	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
1.37	"Software Supporting Materials"	1.38	has the meaning given to it in paragraph 9.1 of this Schedule;
1.39	"Source Code"	1.40	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;
1.41	"Specially Written Software"	1.42	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;
1.43	"Supplier System"	1.44	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. This paragraph 3 applies where the Buyer has conducted a Further Competition. 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 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 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 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 Further Competition, 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 Call Off Contract Period:
 - 6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this 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. Maintenance of the ICT Environment

- 8.1. If specified by the Buyer undertaking a Further Competition, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.
- 8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.
- 8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.
- 8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Supplier: Specially Written Software

- 9.1.1. 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:
 - 9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
 - 9.1.1.2. 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**").
- 9.1.2. The Supplier shall:

- 9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
- 9.1.2.2. 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
- 9.1.2.3. without prejudice to paragraph 9.1.2.2, 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.
- 9.1.3. 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.
- 9.2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**
 - 9.2.1. 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
 - 9.2.2. 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 Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.
 - 9.2.3. 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 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. 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

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.2 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.

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

9.3.1. 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.

9.3.2. 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.

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee 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.

9.3.4. 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:

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

9.3.4.2. will no longer be made commercially available

9.4. Buyer's right to assign/novate licences

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. 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.

- 9.4.2. 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 9.2.

9.5. Licence granted by the Buyer

- 9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written 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).

9.6. Open Source Publication

- 9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) 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:

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

9.6.1.2. based on Open Standards (where applicable),

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

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

9.6.2.1. 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;

9.6.2.2. 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;

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

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

9.6.2.5. 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

9.6.2.6. do not contain any Malicious Software.

- 9.6.3. 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:

- 9.6.3.1. 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
- 9.6.3.2. 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.

9.7. Malicious Software

- 9.7.1. 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.
- 9.7.2. 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.
- 9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:
 - 9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied 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 Buyer when provided to the Supplier; and
 - 9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. Supplier-Furnished Terms

10.1. Software as a Service Terms

- 10.1.1.1. Additional terms for provision of a Software as a Service solution are detailed in Annex D of this Call-Off Schedule 6.

(a)

11. CUSTOMER PREMISES

11.1 Licence to occupy Customer Premises

- 11.1.1 Any Customer 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 Call- Off Contract. The Supplier shall have the use of such Customer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Call-Off Contract [and in accordance with Call-Off Schedule 10 (Exit Management)].

11.1.2 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 Call-Off 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.

11.1.3 Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of this Call-Off Schedule 6 and set out in the Order Form (or elsewhere in this Call Off 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 paragraph 11.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

11.1.4 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.

11.1.5 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 this Call-Off Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

11.2 Security of Buyer Premises

11.2.1 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.

11.2.2 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.

12. Buyer Property

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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 this Call-Off Contract and for no other purpose without Approval.

12.6 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 with Call- Off Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.

12.7 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.

13. Supplier Equipment

13.1 Unless otherwise stated in this Call Off Contract, the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

13.2 The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

13.3 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 Call-Off 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.

13.4 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.

13.5 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 Call Off Contract, including the Service Levels.

13.6 The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

13.7 The Supplier shall, at the Buyer's written request, at its own expense and as soon as reasonably practicable:

13.7.1 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 this Call-Off Contract; and

13.7.2 replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.

ANNEX A

Non-COTS Third Party Software Licensing Terms

None-TBC

ANNEX B

COTS Licensing Terms

None-TBC

ANNEX C

Software Support & Maintenance Terms

None-TBC

ANNEX D

Software as a Service Terms

Maven SAAS Terms and Conditions Agreement

This Maven SAAS Agreement ("Agreement") is entered into as of the [REDACTED], 2020 (the "Effective Date") by and between Conduent Public Health Solutions, Inc. incorporated under the laws of State of Delaware with an address for the purposes of this Agreement at Conduent Public Health Solutions, 12357 Riata Trace Pkwy., Building 5, Ste. 300, Austin, TX 78727 ("Conduent") and [REDACTED] ("Licensee") with an address for the purposes of this Agreement at [REDACTED].

WHEREAS, CONDUENT developed certain code and related documentation as specified in Section 1.1 and 2.1 ("Licensed Code" and "Documentation", respectively);

WHEREAS, Licensee desires to license the compiled Licensed Code for electronic application and decision support activities; and

WHEREAS, CONDUENT is willing to license the Licensed Code to Licensee subject to the following terms and conditions and once agreed upon license fee is paid in full.

NOW THEREFORE, the parties hereby agree as follows:

1. GRANT OF LICENSES

- 1.1 The Licensed Code and Documentation are subject to copyright and other intellectual property rights. No ownership interest in the Licensed Code or documentation is transferred to Licensee hereunder, it being agreed that the Licensed Code and Documentation are being licensed and not sold to Licensee.

CONDUENT hereby grants to Licensee, and Licensee hereby accepts, a worldwide, non-exclusive, non-transferable, and limited copyright license to use, execute, display, copy, merge, compile and internally distribute the Licensed Code (Maven 6.1), for use only for Licensee's [REDACTED] purpose ("Purpose") on at most 1 production instance (clustered or unclustered), 1 test instance, 1 staging instance and 1 development instance within [REDACTED] ("Jurisdiction") in the licensee's address above. Please note that there is a limit of [REDACTED] users on the production system and these users must be based in the Jurisdiction.

- 1.2 CONDUENT further grants to Licensee a worldwide, non-exclusive, non-transferable and limited license to access, use, display and copy the Documentation for Licensee's users only (and only users within the state specified in licensee's address above) in order to utilize the Licensed Code consistent with the licenses granted herein.
- 1.3 Licensee acknowledges that, except for the express copyright license granted herein to the Licensed Code and Documentation no other rights, immunity or license of any kind whether expressed or by implication, estoppels or otherwise, are hereby granted with respect to any patent, trademark, copyright, mask work, trade secret or other intellectual property rights of CONDUENT.

2.0 SAAS CLOUD HOSTING SERVICES

- 2.1 Hosting services as defined in Appendix A.

3.0 LICENSEE RESPONSIBILITIES

- 3.1 Licensee may make only as many machine-readable and/or printed copies of the Licensed Documentation as are reasonably necessary to support Licensee's exercise of its rights under Section 2.0. Licensee may use the Licensed Code on only one instance (clustered or un-clustered) and solely for the Purpose. Licensee will not remove any CONDUENT copyright notices and/or other notice of proprietary rights appearing in the Licensed Code or Documentation in any copies.

- 3.2 Licensee may not reverse assemble, reverse compile, or otherwise translate the Licensed Code except as specifically permitted by law without the possibility of contractual waiver.
- 3.3 Licensee agrees to make its best efforts to ensure that reference is made to the CONDUENT in any communication or publication related to the use of the Licensed Code or Documentation.

4 WARRANTY

- 4.1 LICENSOR IS LICENSING THE LICENSED CODE AND THE DOCUMENTATION ON AN "AS IS" BASIS AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF NON-INFRINGEMENT OR ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. LICENSOR DOES NOT WARRANT THAT THE LICENSED CODE WILL OPERATE IN COMBINATION WITH ANY LICENSEE CODE, OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT THE LICENSED CODE OR DOCUMENTATION WILL MEET LICENSEE'S, OR ITS LICENSEE'S REQUIREMENTS.

5 TERM OF LICENSE

- 5.1 This Agreement shall become effective as of the "Effective Date" set forth above.
- 5.2 Licensee may terminate this Agreement on sixty (60) days prior written notice to CONDUENT. No refunds of any licensing fees will be made by Conduent to Licensee unless otherwise agreed upon in writing in a formalized Letter of Agreement or contract pursuant to a Request for Proposal or Request for Quote or Request for Offer.
- 5.3 If Licensee materially breaches a term of this Agreement, CONDUENT may, at its option, terminate this Agreement provided the Licensee is given written notice and fails to cure such breach within thirty (30) days. Notwithstanding the foregoing, CONDUENT may terminate this Agreement immediately if it has a reasonable basis to believe any of the Licensed Code or Documentation licensed under this Agreement infringes an intellectual property right of any third party.

6 PRICING

- 6.1 Pricing shall be based on: XXXXXXXX
- 6.2 RESERVED.
- 6.3 Licensee may request professional services for additional project management, training or technical work. If such services are requested, they will be provided by CONDUENT at a rate of XXXXXX per hour. All such additional services shall be detailed in a Task Order containing any and all pertinent information and total price (the "Task Order") that will be attached hereto and incorporated herein. All Task Orders must be in writing and signed by both parties.

7 PAYMENT TERMS

- 7.1 Licensee shall remit prompt and proper payment to CONDUENT for all invoiced amounts due within thirty (30) calendar days from the receipt thereof. Licensee's failure to promptly pay CONDUENT for all invoiced amounts shall be considered a material breach of this Agreement and may result in termination in accordance with Section 4.0 of this Agreement.
- 7.2 RESERVED.

8 LIMITATION OF REMEDIES

- 8.1 CONDUENT's entire liability and Licensee's exclusive remedy are set forth in this Section 7.0.
- 8.2 CONDUENT's liability for damages to Licensee for any cause(s) whatsoever and regardless of the form of action shall be limited in the aggregate to 50% percent of the amount of license fee paid to CONDUENT by Licensee.
- 8.3 Under no circumstances will CONDUENT be liable for any damages caused by Licensee's failure to perform its obligations under this Agreement, or for any third party claims, special, incidental, punitive or indirect damages, or for any consequential damages, including lost opportunities, profits and savings, even if informed of their possibility.

- 8.4 Licensee shall be solely liable for any claims based on its use of and/or modifications of the Licensed Code in violation of the terms of this Agreement, including any damages caused by the Licensee's failure to perform its responsibilities under this Agreement. Licensee shall indemnify and hold CONDUENT harmless from any cause of action brought by any party against CONDUENT resulting from the Licensee's use of Licensed Code contrary to the terms of this Agreement.

9 PERSONALLY IDENTIFIABLE INFORMATION and DATA

- 9.1 Licensee understands and agrees that the provisions of the Privacy Act of 1974, as amended; the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended; and all other federal, State, and local privacy laws, ordinances, and regulations specifically apply to the Purpose provided under this Agreement and the obligations of Licensee under the "Compliance With Laws and Regulations" Section of this Agreement.
- 9.2 The Licensee will retain title to and all ownership rights in all data provided by the Licensee and its Users (the "Data"), but grants CONDUENT the right to access and use Data solely for the purpose of complying with its obligations under this Agreement.

10 COMPLIANCE WITH LAWS AND REGULATIONS

- 10.1 Licensee acknowledges that certain local, State, and federal laws and regulations apply to the Licensee. Licensee agrees to comply with all applicable federal, State, and local laws and regulations in effect during the Term of this Agreement as it relates to the Hosted Software. To the extent permitted by law, Licensee agrees to defend, indemnify, and hold CONDUENT (and the parent, affiliates, subsidiaries, employees, directors, officers, and agents of CONDUENT) harmless against all claims, damages, losses, causes of action, liabilities, and expenses of any kind or nature, including reasonable attorney fees, that are due to, arise out of, or are incident or related to the failure of Licensee to comply with applicable laws and regulations during the the Term of this Agreement.

11 RELATIONSHIP OF THE PARTIES

- 11.1 This Agreement shall not constitute, create, give effect to, or otherwise imply a joint venture, partnership, or business organization of any kind. CONDUENT and Licensee are independent parties, and neither party shall act as an agent for or partner of the other for any purpose. Nothing in this Agreement shall grant to either party any right to make any commitments of any kind for or on behalf of the other party without the prior written consent of the other party. Licensee shall not be restricted from performing any business activity for others and shall not be bound to CONDUENT except as provided under this Agreement.

12 NOTICES

- 12.1 Unless otherwise specified in this Agreement, all notices, requests, or consents required to be given in writing under this Agreement shall be hand delivered, delivered by overnight delivery service, or mailed (certified mail, postage prepaid), to the party indicated on the signature page (with a delivery receipt requested), unless that party notifies the other, in writing, of a change in the address or contact information:

To CONDUENT:

Conduent Public Health Solutions, Inc.

12357 Riata Trace Pkwy., Building 5, Ste. 300

Austin, TX 78729

Attn: Legal Department

To Licensee:

Attn:

13 FORCE MAJEURE

- 13.1 CONDUENT shall not be liable to Licensee for any failure, delay or disruption of any services or access to the software caused by a Force Majeure Event, whether or not such matters were foreseeable, and such failure or delay shall not constitute a material breach of this Agreement. A "Force Majeure Event" means any cause beyond the reasonable control of CONDUENT that could not, by reasonable diligence, be avoided, including acts of God, acts of war, terrorism, riots, embargoes, disease, pandemics, acts of civil, government or military authorities, and any other acts beyond the reasonable control of CONDUENT, including but not limited to flood, snow, fire, hurricane, earthquake, accident or strike.

14 GENERAL PROVISIONS

- 14.1 The validity, construction and performance of this Agreement will be governed by the substantive laws of the State of New York, United States, as though this Agreement were executed in and fully performed within the State of New York and without regard to any conflict of laws provisions. Neither party will bring a legal action against the other more than one (1) year after the cause of action arose. Both parties waive the right to a jury trial in any dispute arising out of this Agreement. Both parties agree that any action concerning this Agreement shall be brought in a court of competent jurisdiction in the State of New York and hereby consent to the jurisdiction of any such court and to service of process in the manner provided for the giving of notices pursuant to this Agreement.
- 14.2 If any part, term or provision of this Agreement is declared unlawful or unenforceable by a court of competent jurisdiction, the remainder of this Agreement shall remain in full force and effect. The headings contained in this Agreement are for reference purposes only and shall not affect in any way the meaning or interpretation of this Agreement.
- 14.3 Except with the prior written consent of CONDUENT, Licensee may not (a) assign or transfer (whether by merger, consolidation, acquisition, change of control, operation of law, or otherwise) this Agreement or any of its rights under this Agreement; or (b) delegate or subcontract any of its duties or obligations under this Agreement.
- 14.4 Nothing in this Agreement grants either party any rights to use the other party's trademarks or trade names, directly or indirectly, in conjunction with any product, service, promotion, publication or publicity without prior written approval of the other party or trademark or trade name owner.
- 14.5 Each party agrees to comply, at its own expense, with all applicable federal, state, and local laws, rules, regulations, orders, and ordinances relating to the export of technical data, insofar as they relate to activities allowed or to be performed under this Agreement.

15 ENTIRE AGREEMENT

- 15.1 The contents of this Agreement (any other schedules or attachments to this Agreement that are referred to and incorporated in this Agreement by reference) constitute the entire understanding and Agreement between the parties with respect to the License and supersede any prior agreements, written or oral, related to the License that are not specifically referenced and incorporated in this Agreement. The terms and conditions of this Agreement shall not be changed or modified except by written amendment signed by both parties.

THE PARTIES ACKNOWLEDGE THAT EACH HAS READ THIS AGREEMENT AND ITS ATTACHMENTS, UNDERSTANDS THEM, AND AGREES TO BE BOUND BY THEIR TERMS AND CONDITIONS. FURTHER, THE PARTIES AGREE THAT THIS AGREEMENT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES WHICH SUPERSEDES ALL PROPOSALS AND ALL PRIOR AGREEMENTS, ORAL OR WRITTEN, AND ALL OTHER COMMUNICATIONS BETWEEN THE PARTIES RELATING TO THE SUBJECT MATTER HEREOF.

Conduent Public Health Solutions, Inc. Licensee
ACCEPTED AND AGREED TO: ACCEPTED AND AGREED TO:

By: _____

By: _____

Print Name: _____ Print Name: _____

Title: _____ Title: _____

Date: _____ Date: _____

Appendix A-SaaS Hosting Services

2.0 SAAS CLOUD HOSTING SERVICES	55
2.1 Hosting services as defined in Appendix A.....	55
Overview.....	59
Azure	59
SaaS Hosting System Availability.....	61
Azure Components	62
OSSEC	63
Anti-virus Software.....	63
Automated Backup and Recovery Software	63
System Audit Trail Logs	63

Overview

Below is a generic description of the proposed hosting specifications for the cloud hosting deployment of Maven. Conduent reserves the ability to revise the specifications based on further analysis with PHE.

Azure

Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. It provides software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) and supports many different programming languages, tools, and frameworks, including both Microsoft-specific and third-party software and systems. Conduent, Inc. has approved this vendor's IaaS offerings for deploying production instances of Maven as a low-cost yet highly performant alternative to traditional dedicated hosting methods.

HOSTING: Azure CLOUD RECOVERY

OBJECTIVES:

Recovery Point Objective: 8 business hours
Recovery Time Objective: 24 business hours

BANDWIDTH

Unlimited Outbound Transfer
Unlimited Inbound Transfer

AVAILABILITY MONITORING

Servers checked every minute for availability
All exposed URLs checked every 30 seconds by multiple agents for responsiveness

SECURITY THREAT MANAGER

Order Form & Schedules

Public Health England: Public Health Infectious Disease Case and Incident Management System

ConfigServer Security & Firewall provides stateful packet inspection (SPI), login/intrusion detection (IDS), and operating system level security on application servers.

SSL SECURITY CERTIFICATE1

Sectigo RSA SSL Certificate

FIREWALL

Servers run in an Azure Virtual Private Cloud (VPC) with separate public and private subnets for application servers and database servers respectively
Full access control list (ACL) permissions per virtual subnet
All ports blocked until explicitly opened on a per-server basis

VPN ACCESS

IPSec Hardware or Software VPN access available at additional cost per connection

AZURE LOAD BALANCER

Load Balancing (ELB)
SSL support

EXAMPLE APPLICATION SERVER(S)

Azure Kubernetes Service (AKS)
EC2 Instance Type: gp.r5.2xlarge2
Processor: 3.4 GHz Intel Xeon® Platinum 8272CL Hyper Thread configuration Xeon Processors – 8 cores
Memory: 32 GB

Managed OS Disks – S15

Storage: 200 GB

Storage: Highly replicated SSD backed Elastic Block Storage (EBS) – 200GB

EXAMPLE BATCH SERVER(S)

EC2 Instance Type: gp.r5.2xlarge2
Operating System: Windows Server
Processor: 3.4 GHz Intel Xeon® Platinum 8272CL Hyper Thread configuration Xeon Processors – 8 cores
Memory: 32 GB
2 managed Disks – P15
Storage: 400 GB
Storage: Highly replicated SSD backed Elastic Block Storage (EBS) – 200GB

EXAMPLE FILE SERVER(S)

EC2 Instance Type: gp db.r5.2xlarge2
Operating System: Windows Server
Processor: 3.4 GHz Intel Xeon® Platinum 8272CL Hyper Thread configuration Xeon Processors – 4 cores
Memory: 16 GB
Storage: 200 GB

EXAMPLE OPERATIONAL DATABASE SERVER

Azure RDS for MySQL
RDS Instance Type: gp.db.r5.2xlarge
Processor: 8 vCPUs
Memory: 32 GB
Storage: 3 TB
Backup: GRS redundancy

EXAMPLE REPORTING DATABASE SERVER

Azure RDS for MySQL
RDS Instance Type: gp.db.r5.2xlarge
Processor: 8 vCPUs
Framework Ref: RM6068
Project Version: v0.1
Model Version: v3.2, Crown Copyright

Memory: 32 GB
Storage: 3 TB
Backup: GRS redundancy

DISASTER RECOVERY

This cloud-based system is designed from the ground up to be inherently durable with a quick turnaround time in case of disaster. Application servers do not hold any data other than the application itself and therefore can be replaced with new instances in case of disaster. Additionally, application servers run in a cluster so if one fails, the load is taken by others in the cluster all while the failed server is recovered and re-added. The operational database has a secondary server in a separate availability zone already running as a replica, so in the event the primary server fails the service will continue to run seamlessly on the secondary server while the primary is rebuilt automatically. In the scenario of an entire Azure region failure, daily incremental snapshots of the operational database are sent to a different region.

SaaS Hosting System Availability

SYSTEM PERFORMANCE	
Service Metric	The system shall maintain an uptime (be operationally available) for at least 99.5%. Monthly System Availability/Uptime Report will be shared with PHE.
Description	<p>System Performance times will be measured by capturing the timing of the synthetic transactions listed below using a Synthetic Monitoring tool:</p> <ul style="list-style-type: none"> - Create a Case - Update a Case - Lookup a Case - Lookup a Person. <p>The time the requests were initiated until the time the responses are received will be recorded and used to report response time.</p> <p>Inquiry transactions will be performed by providing a valid record identifier(s). Conduent will select the parameters for the transaction in consultation with Customer.</p> <p>Please Note: The transactions listed above do not represent the entire scope of Maven. Should a transaction not listed above encounter performance responses which do not meet the Service Level criteria, a Jira ticket will be opened, and Conduent will correct the problem in a mutually agreed time frame as per the Support levels agreed upon.</p>
Measurement Interval	Every 15 minutes during business hours (Exclusions apply and are noted below).
Reporting Period	Monthly (Data will be captured as per the Measurement Interval and accumulated monthly for the Service Level performance report).

Exclusions	<ul style="list-style-type: none"> - Service level will not be applicable during maintenance and batch schedule windows. - Service level will not be applicable during deployments, batch runs, data refresh, and any ad hoc/on demand data load, Queries, reports or other resource intensive batch jobs like full Denormalization table loads. - Service level will not be applicable in the event of any slowness/outages caused by third party vendor code or infrastructure (e.g. Amazon.) will be excluded from the Service level calculation. - Service level will not be applicable in the event of any slowness/outages due to hardware/network/ connectivity or other infrastructure/desktop issues. - Service level will not be applicable in the event of any slowness/outages caused due to configuration changes made in Maven by PHE. - Monitoring Counters will exclude network latency and user login time from the performance Service Level calculation. - Conduent will have 60 days after any new deployment to stabilize and tune the system configuration to meet the SLA.
------------	--

Azure Components

- Azure Web Services Regions and Availability Zones (AZs): Azure Web Services is divided into separate geographical regions, each with distinct availability zones (AZs). Most Azure services provide some level of cross-AZ backup/failover support, such as automated RDS backups from one AZ to another AZ within the same region.
- Azure Virtual Machines (Azure VMs): Azure VM provides the virtualization layer of the infrastructure. Virtual servers run within VM and provide the operating environment for the Java EE web application servers to run in. VM provides virtual CPU cores, memory, and hard disks and is the core of the IaaS platform. The recommended configuration for VM is an gp.r5.2xlarge2 instance running Linux. The gp.r5.2xlarge2 configuration consists of 8 virtual CPUs, 15 GB of memory, and 2x40 GB of SSD storage (total raw storage of 200 GB in a RAID 1 configuration).
- Azure Load Balancer (ELB): An Azure load balancer is a Layer-4 (TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs. A load balancer health probe monitors a given port on each VM and only distributes traffic to an operational VM.
- Azure Blob Storage: Azure blob Storage provides back-end, persistent block level storage volumes that are automatically replicated within their AZ (availability zone). EBS is used as a transparent, back-end storage solution in both VMs and RDS services.
- Azure Relational Database Service (Azure RDS): RDS provides the virtual database service component of the infrastructure. RDS is preferable over traditional database hosting options due to built-in automation of standard database operations, including automated backups, auto DB snapshots, read-replica capability (ideal for Maven reporting database functionality), and multi-AZ deployment and fail-over functionality. Azure MySQL is the standard, recommended configuration for RDS. Note that supports full end-to-end encryption, including both encryption-at-rest and encryption-in-transit. More information about RDS can be found at the following link: [Seamlessly deploy RDS with ARM and Azure Marketplace | Microsoft Docs](#).
- Azure DNS, Azure Traffic Manager: Azure DNS is a cloud based DNS web service for configurable, dynamic routing of web services and can be used as an alternative to traditional DNS services. Note that Azure DNS handles DNS requests and does not have access to any actual Maven data.
- Azure Monitor: Azure Monitor is a monitoring service for Azure cloud resources and application. Azure monitor is used for database and application monitoring. Disk space monitoring is enabled on application server through cloud watch client. Disk space and DB connection monitoring is enabled on database server. Alerts has been setup and tested. Email alerts will be sent if the disk uses on EBS volume is greater than or equals to 90 %, DB space is less than 20 GB and DB connection is more than

Order Form & Schedules

Public Health England: Public Health Infectious Disease Case and Incident Management System

30000. Endpoint URL response time is also monitored and alerts if the response time is more than 10 seconds. Alerts will be sent out to IT Support. It has been tested by creating false positive alerts lowering or increasing the alert levels.

- Azure DB Audit logging and Integrity monitoring: - Advanced logging has been enabled to record and audit database any events and errors. Audit/error logs sent by the Databases are captured by Cloud watch log and parsed for any discrepancies like login failure event, DB drop event etc. which then creates an alarm and notifies the respective parties accordingly. Alert has been tested and validated by creating sample DB events deliberately like multiple login attempt, table modification etc. in a test environment.
- Azure Backup and Restore Service: Azure has a fully managed centralize and automated backup service that will help to meet business and regulatory backup compliance requirement. Azure backup service will centrally configure backup policies and monitor backup activity for Azure cloud resources. Azure backup policies will allow to schedule monthly backup with the indefinite retention period. Restore of database will take couple of hours. Backup and restore process has been tested on dev environment successfully.

OSSEC

OSSEC is an open source tool used for host-based intrusion detection system (HIDS) monitoring. OSSEC will detect attacks, misuse or system errors using logs as primary source of information and will notify through the alert. OSSEC has master server which will collect data from its agent nodes and send alerts based on the collected information. OSSEC agents are installed in EC2 nodes and logs the event sent by the agents which will notify IT Support for any file permission changes, file deletion, file addition, file content update etc. The setup has been tested modifying the files and sending the false positive alerts in test node.

Anti-virus Software

The following screenshots show anti-virus software running on the servers.

```
root@node1:~# service clamav-freshclam status
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2019-04-27 07:00:30 CDT; 2 months 1 days ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://www.clamav.net/documents
   Main PID: 1093 (freshclam)
   CGroup: /system.slice/clamav-freshclam.service
           └─1093 /usr/bin/freshclam -d --foreground=true
```

```
ubuntu@node2:~$ sudo service clamav-freshclam status
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2019-04-27 07:25:40 CDT; 2 months 0 days ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://www.clamav.net/documents
   Main PID: 1067 (freshclam)
    Tasks: 1
   Memory: 256.2M
      CPU: 16min 53.059s
   CGroup: /system.slice/clamav-freshclam.service
           └─1067 /usr/bin/freshclam -d --foreground=true
```

Automated Backup and Recovery Software

Automated backups are taken of the application servers and production databases and kept for 30 days.

System Audit Trail Logs

Maven provides an audit trail for all event management activity. The audit trail logs are stored in the encrypted production database. The audit trail captures the following information:

- Timestamp – When did the auditable event occur
- Case Type – Type of the auditable event, e.g., event created, questionnaire updated, contact added, event closed
- Details – Details associated with the auditable event, e.g., which contact was added

Framework Ref: RM6068

Project Version: v0.1

Model Version: v3.2, Crown Copyright

- Username – User who performed the activity

The event activity audit trail is stored in the database and is visible to authorized users through the web user interface and through reports. The granularity of the event specific auditable events can vary from event creation to updates to a particular data field (individual form fields can be marked as auditable).

In addition to capturing all updates in the event level audit trail, the Maven EDSS audit trail captures all read and administrative access to the system, which is important for HIPAA compliance. This audit trail includes the following activities:

- Searches – Any searches performed by users will be captured in the audit trail.
- Case Access – When a user opens an existing event from search results or from a workflow queue, this activity will be logged in the view activity audit trail.
- Reports – When a user runs a report this activity will be logged in the view activity audit trail.
- Administrative Actions - Examples of these actions include creating and modifying user profiles, groups, roles, workflows and reports.

The non-event specific activity audit trail is also captured in the Maven database, and access to this audit trail is supported through a parameterized report, which will allow authorized users to view the audit trail contents based on the given criteria (e.g., start date, end date, audit event type, username etc.).

Annex E

Device as a Service Terms

None-TBC

Joint Schedule 6 (Key Subcontractors)

2. Restrictions on certain subcontractors

- 2.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.
- 2.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.
- 2.3 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 section 20 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to 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:
 - 2.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 2.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 2.3.3 the proposed Key Subcontractor employs unfit persons.
- 2.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - 2.4.1 the proposed Key Subcontractor's name, registered office and company registration number;
 - 2.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
 - 2.4.3 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;
 - 2.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
 - 2.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and
 - 2.4.6 the Dun & Bradstreet Failure Rating score of the Key Subcontractor.
- 2.5 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:
 - 2.5.1 a copy of the proposed Key SubContract; and

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

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

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

2.6.2 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;

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

2.6.4 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;

2.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework 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);

2.6.6 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

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.

Call-Off Schedule 7 (Key Supplier Staff)

- 2.7 1.1 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.
- 2.8
- 2.9 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 2.10
- 2.11 1.3 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.
- 2.12
- 2.13 1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
- 2.14
- 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
 - 1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
- 2.15 1.5 The Supplier shall:
- 1.5.1 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);
 - 1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
 - 1.5.3 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 one (1) Month notice;
 - 1.5.4 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
 - 1.5.5 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.

- 1.6 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.

Annex 1- Key Roles

Key Role	Key Staff	Contract Details
User Researcher / Business Analyst / Training Lead	[REDACTED]	
Service Designer / Technical Architect	[REDACTED]	
Senior Developer	[REDACTED]	
Test Lead	[REDACTED]	
Delivery Manager	[REDACTED]	
Project Manager	[REDACTED]	
Support Lead	[REDACTED]	
Support Lead	[REDACTED]	
Epidemiologist	[REDACTED]	

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Part B: Short Form Business Continuity & Disaster Recovery

1. The Supplier's business continuity and disaster recovery plan is appended at Annex 1 hereto.
2. The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier if required at no additional cost to the Buyer.
3. If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans

Annex 1

Call-Off Schedule 9 (Security)

Part B: Long Form Security Requirements

3. Definitions

3.1 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: <ul style="list-style-type: none">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/orb) 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.

4. Security Requirements

4.1 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.

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

4.2.1 [REDACTED]

4.2.2 [REDACTED]

4.3 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.

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

4.5 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.

4.6 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.

4.7 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.

5. Information Security Management System (ISMS)

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

5.2 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.

5.3 The Buyer acknowledges that;

5.3.1 If the Buyer has not stipulated during a Further Competition 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

5.3.2 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.

5.4 The ISMS shall:

5.4.1 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;

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

5.4.3 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;

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

5.4.5 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

5.4.6 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).

- 5.5 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.
- 5.6 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.
- 5.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 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.
- 5.8 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.

6. Security Management Plan

- 6.1 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 a draft Security Management Plan which shall comply with the requirements of Paragraph 4.2.
- 6.2 The Security Management Plan shall:
- 6.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
 - 6.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
 - 6.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
 - 6.2.4 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;

- 6.2.5 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;
- 6.2.6 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);
- 6.2.7 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);
- 6.2.8 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;
- 6.2.9 set out the scope of the Buyer System that is under the control of the Supplier;
- 6.2.10 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
- 6.2.11 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.

6.3 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.

6.4 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.

7. Amendment of the ISMS and Security Management Plan

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

- 7.1.1 emerging changes in Good Industry Practice;
- 7.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
- 7.1.3 any new perceived or changed security threats;
- 7.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
- 7.1.5 any new perceived or changed security threats; and
- 7.1.6 any reasonable change in requirement requested by the Buyer.

7.2 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:

- 7.2.1 suggested improvements to the effectiveness of the ISMS;
- 7.2.2 updates to the risk assessments;
- 7.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
- 7.2.4 suggested improvements in measuring the effectiveness of controls.

7.3 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 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

7.4 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.

8. Security Testing

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

9. Complying with the ISMS

9.1 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.

9.2 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.

- 9.3 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.

10. Security Breach

- 10.1 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.

- 10.2 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:

10.2.1 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.

10.3 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.

11. Vulnerabilities and fixing them

11.1 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.

11.2 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:

11.2.1 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

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

11.3 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:

11.3.1 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;

11.3.2 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

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

11.4 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:

11.4.1 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

11.4.2 is agreed with the Buyer in writing.

11.5 The Supplier shall:

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

11.5.2 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;

11.5.3 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;

11.5.4 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 3.3.5;

11.5.5 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;

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

11.5.7 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

11.5.8 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.

11.6 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.

11.7 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

12. Handling Classified information

- 12.1 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.

13. End user devices

- 13.1 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").
- 13.2 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.

14. Data Processing, Storage, Management and Destruction

- 14.1 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.
- 14.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).
- 14.3 The Supplier shall:
- 14.3.1 provide the Buyer with all Government Data on demand in an agreed open format;
 - 14.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

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

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

15. Ensuring secure communications

15.1 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.

15.2 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.

16. Security by design

16.1 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.

16.2 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).

17. Security of Supplier Staff

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

17.2 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.

17.3 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.

17.4 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.

17.5 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.

18.Restricting and monitoring access

- 18.1 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.

19.Audit

- 19.1 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:
- 19.1.1 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.
 - 19.1.2 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.
- 19.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 19.3 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

Time frame to be agreed after initiation.

Call-Off Schedule 10 (Exit Management)

Part B: Short Form Exit Management Requirements

1. Within 20 (twenty) working days of the Start Date the Supplier must provide the Buyer with an exit plan which ensures continuity of service and which the Supplier will follow.
2. The Supplier must ensure that the exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its Replacement Supplier at the expiry or if the contract ends before the scheduled expiry.
3. The exit plan should set out full details of timescales, activities and roles and responsibilities of the Parties for:
 - the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
 - the strategy for export and migration of Buyer data from the Supplier system to the Buyer or a Replacement Supplier, including conversion to open standards or other standards required by the Buyer
 - the transfer of project- specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
 - the testing and assurance strategy for exported Buyer data
 - if relevant, TUPE-related activity to comply with the TUPE regulations
 - any other activities and information which are reasonably required to ensure continuity of Service during the exit period and an orderly transition
4. When requested, the Supplier will help the Buyer to migrate the Services to a Replacement Supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract ended before the Expiry Date due to Supplier cause. Otherwise any additional costs incurred by the Supplier in providing such assistance shall be subject to the Variation Procedure.

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 the other Party is also “Controller”,

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

Where one Party is Controller and the other Party its Processor

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 UK 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 Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a 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 Subprocessor to Process any Personal Data related to the Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which gives 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 17 of this Joint Schedule 11, 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 paragraphs 16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

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

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: [REDACTED]
- 1.2 The contact details of the Supplier's Data Protection Officer are: Contractor (Insight) – [REDACTED] Sub-contractor (Conduent) [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

A) Personal Data Processing Template

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority 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 Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> • Processing Data <ul style="list-style-type: none"> ○ PII Data <ul style="list-style-type: none"> ▪ Name, Address, NHS ID, Email, Phone number, Demographic information ▪ Close Contact details (Persons in contact with) ○ PHI Data <ul style="list-style-type: none"> ▪ Sensitive personal information in the form of Lab test results ▪ Case Questionnaire Data (Clinical data, Symptoms, Infectious Dates, Reporting Facilities, etc. ○ Provider information ○ Facility information (Treatment) <p>The Supplier is Controller and the Relevant Authority is Processor The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:</p> <ul style="list-style-type: none"> • Not Applicable <p>The Parties are Joint Controllers The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> • Not Applicable

Duration of the Processing	Conduent duration of processing is 27-September 2021 to 26-September 2026.								
Nature and purposes of the Processing	Buyer is implementing Maven As a SaaS Solution. Conduent will be responsible for the implementation and data migration (strategy and mapping only) for the Maven solution. As part of the implementation, data may be shared with Conduent for the purpose of testing the data as part of the implementation, post go-live support as per the Implementation Plan and Deliverables.								
Type of Personal Data	<p><i>[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]</i></p> <table border="1"> <thead> <tr> <th>Data Category</th><th>Data Description</th></tr> </thead> <tbody> <tr> <td>Party Information</td><td> <ul style="list-style-type: none"> Person information - (PII & PHI Data (Name, Address, NHS ID, Email, Phone number, Demographic information)) Contact person Information </td></tr> <tr> <td>Case Information</td><td> <ul style="list-style-type: none"> Provider and Facility Information Sensitive personal information in the form of Lab test results Close Contact information </td></tr> <tr> <td></td><td></td></tr> </tbody> </table> <p>For a complete list please see below link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/</p>	Data Category	Data Description	Party Information	<ul style="list-style-type: none"> Person information - (PII & PHI Data (Name, Address, NHS ID, Email, Phone number, Demographic information)) Contact person Information 	Case Information	<ul style="list-style-type: none"> Provider and Facility Information Sensitive personal information in the form of Lab test results Close Contact information 		
Data Category	Data Description								
Party Information	<ul style="list-style-type: none"> Person information - (PII & PHI Data (Name, Address, NHS ID, Email, Phone number, Demographic information)) Contact person Information 								
Case Information	<ul style="list-style-type: none"> Provider and Facility Information Sensitive personal information in the form of Lab test results Close Contact information 								
Categories of Data Subject	<p>Includes:</p> <ul style="list-style-type: none"> i). PHE staff, Data Entry Staff, Users & providers using the provider portal concerned with management of the Framework Agreement ii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract iv. Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Contract <p>For a complete list please see below link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/</p>								
Plan for return and destruction of the data once the Processing is complete	All relevant data to be deleted is the responsibility of the Buyer under Framework Contract as they are the owner and controller of the data.								

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A – Implementation Plan

1. Agreeing the Implementation Plan

- 1.1 The Supplier's tendered draft Implementation Plan is at Annex 1 to this Part A of Call-Off Schedule 13. The Supplier will provide an updated, fully developed draft for Buyer's Approval within 20 Working Days of the Call-Off Contract Start Date.
- 1.2 The updated draft must contain enough detail for effective management of Contract implementation.
- 1.3 The Buyer shall work with Supplier to finalize the Approved Implementation Plan. The Buyer shall not unreasonably delay providing its input, the Supplier shall not unreasonably delay incorporating the Buyer's reasonable input, and the Buyer shall not unreasonably delay approving the Approved Implementation Plan. The Parties agree that delays associated with the finalization of the Approved Implementation Plan may result in changes to the Pricing Schedule or other parts of the Contract under the Variation Procedure.

2. Following the Implementation Plan

- 2.1 The Supplier shall perform its obligations in respect of Delivery and, where relevant, Testing of the Deliverables in accordance with the Approved Implementation Plan.
- 2.2 Changes to any Milestones, Milestone Dates, Milestone Payments or Delay Payments shall only be made via the Variation Procedure.
- 2.3 Where the Supplier is solely responsible for the failure to achieve a Milestone by the date specified in the Approved Implementation Plan this shall constitute a Default. Where the Buyer is solely responsible for failure to achieve a Milestone by the date specified in the Approved Implementation Plan, this will not constitute a default by the Supplier and shall, unless otherwise agreed to by both Parties, entitle Supplier to an increase in Milestone Payment amounts and a revision of the Milestone Dates in the Approved Implementation Plan under the Variation Procedure. Where both parties are jointly responsible for the failure to achieve a Milestone by the date specified in the Approved Implementation Plan, then such a failure shall not constitute a default by Supplier and shall, unless otherwise agreed to by the Parties, result in the negotiation of future Milestones under the Variation Procedure.

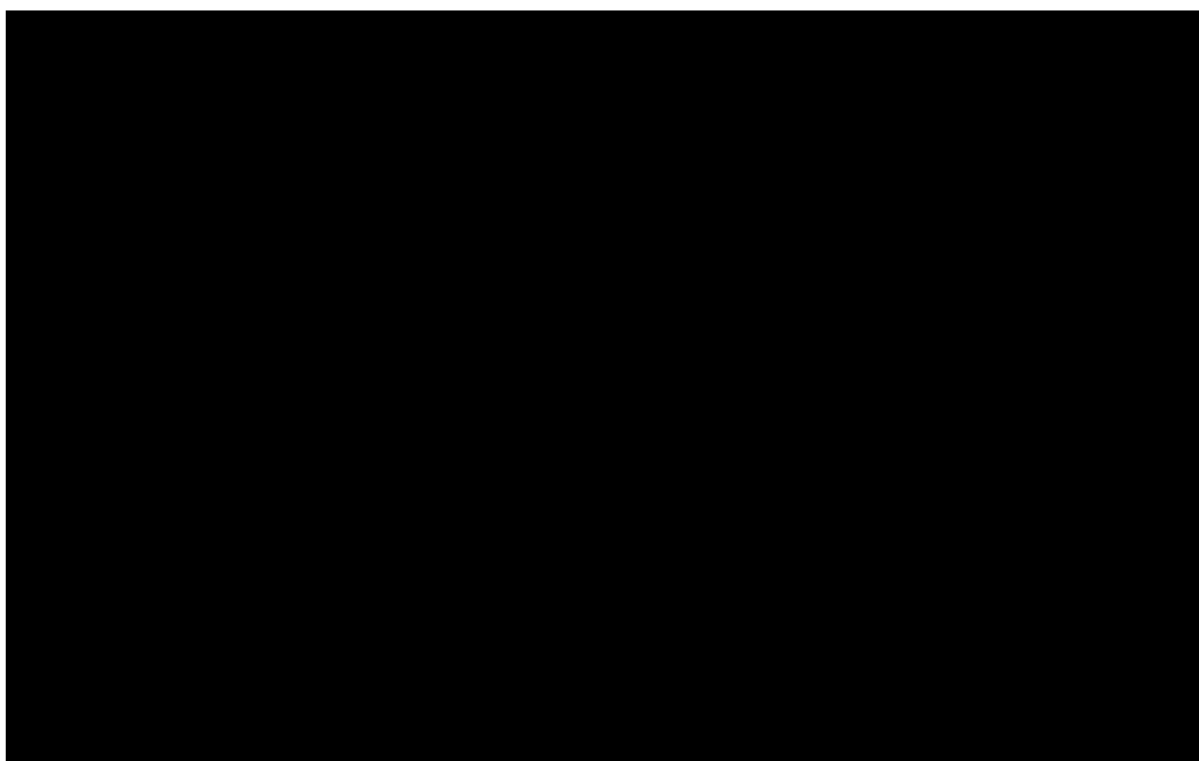
3. Delays

- 3.1 If the Supplier becomes aware that there is, or is likely to be, a Delay it shall;
- Notify the Buyer in writing within 2 Working Days of becoming aware, explaining the likely impact of the Delay
 - Use all reasonable endeavours to mitigate the effects of the Delay, including complying with the Buyer's reasonable instructions

4. Delay Payments

- 4.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date due solely to the fault of the Supplier, the Supplier shall pay to the Buyer the Delay Payments set out in the Contract and the following provisions shall apply:
- Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to achieve a Milestone by its Milestone Date except where:
 - (a) the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or
 - (b) the delay exceeds the number of days (the "Delay Period Limit") specified in the Contract commencing on the relevant Milestone Date;
 - the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is achieved;
- 4.2 [Insert details of Delay Payment rate and Delay Period Limit]

Annex 1 Draft Implementation Plan



Part B – Testing

In this Part B to Call-Off Schedule 13, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Test Plan"	a plan for the Testing of the Deliverables to demonstrate compliance with Contract requirements;
"Test Report"	a test report produced by the Supplier in accordance with Paragraph 3.3 of this Part B to Call-Off Schedule 13;

- 1.1 All Tests will be carried out in accordance with the Test Plan.
- 1.2 The Supplier shall submit each Deliverable for the relevant Testing no later than the date specified in the Test Plan.
- 2.1 The Supplier shall submit a draft Test Plan for Approval no later than 20 Working Days after the Start Date.
- 2.2 The Test Plan will include:
 - An overview of how Testing will be carried out
 - Specific details of each Test to be carried out to demonstrate that the Buyer's requirements are satisfied
 - The Test Success Criteria for all Tests
 - Buyer's involvement in testing (i.e, User Acceptance Testing)A timetable for Testing over the Test Period, this to be compliant with any Implementation Plan
 - The process for recording the conduct and results of Testing
 - The responsibilities of the Parties
 - A categorisation scheme for test issues e.g. critical/serious/minor
- 2.3 Buyer work with Supplier to finalize the Test Plan. The Buyer shall not unreasonably delay providing its input, the Supplier shall not delay in incorporating the Buyer's reasonable input, and the Buyer shall not delay in approving the Test Plan. The Parties agree that delays associated with the finalization of the Approved Test Plan may result in changes to the Pricing Schedule or other parts of the Contract under the Variation Procedure.
- 3.1 Unless specified in the Test Plan the Supplier shall be responsible for carrying out the Testing detailed in the plan.
- 3.2 The Buyer may require that a Buyer representative witnesses the conduct of the Tests.

- 3.3 No later than 20 working days after the completion of the scheduled Test Period the Supplier shall provide the Buyer with a Test Report setting out:
- An overview of Testing carried out
 - Details of each Test carried out together with the result, indicating if the success criteria were satisfied
 - Details of any scheduled Tests that were not carried out
 - A list of all outstanding Test issues
- 4.1 Whereby the end of the scheduled Test Period the Testing process has demonstrated to the Buyer's satisfaction that the Test Success Criteria have been met then the Buyer shall notify the Supplier in writing that the Testing process has been satisfactorily completed.
- 4.2 Where solely as a result of a Supplier default the Testing process has not by the end of the scheduled Test Period demonstrated to the Buyer's satisfaction that the Test Success Criteria have been met then the Buyer may:
- Direct the Supplier to repeat any unsuccessful Test or undertake any scheduled Test not thus far undertaken to give the Supplier an opportunity to demonstrate that the outstanding issues detailed in the Test Report have been resolved; or
 - Notify the Supplier that testing has been satisfactorily completed subject to rectification of outstanding issues within a period specified by the Buyer. Failure to rectify the relevant issues within the period specified shall be a material Default; or
 - to reject the relevant Deliverables and to invoke Clause 3.2.12; or
 - to reject the relevant Deliverables treating this as a material default and invoking the Buyer's termination right under Clause 10.4.1

Call-Off Schedule 14 (Service Levels)

Definitions

In this Part Call-Off Schedule 14, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Critical Service Failure"	Means a failure to meet a Service Level Threshold in respect of a Service Level
Performance Monitoring Report	Means a Performance Monitoring Report as specified by Section 3 of this Call-Off Schedule 14
"Service Credits"	any service credits specified in the Annex to Section 2 of this Call-Off Schedule 14 being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Annex to Section 2 of this Call-Off Schedule 14;
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Section 2 of this Call-Off Schedule 14; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Section 2 to this Call-Off Schedule 14

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

- 20.1 The Supplier shall at all times provide the Deliverables to meet the Service Level Performance Measure for each Service Level.
- 20.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Section 2 to this Schedule 14 including the right to any Service Credits, which are a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.
- 20.3 The Supplier shall send Performance Monitoring Reports to the Buyer in accordance with the provisions of Section 3 (Performance Monitoring) of this Call-Off Schedule 14.

21. Critical Service Level Failure

Not used.

Section 2: Service Levels and Service Credits

1. Service Levels

- 1.1 If the level of performance of the Supplier is likely to or fails to meet any Service Level Performance Measure the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:
- 1.1.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer;
 - 1.1.2 instruct the Supplier to comply with the Rectification Plan Process;
 - 1.1.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
 - 1.1.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits

- 2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.
- 2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Section 2 of this Call-Off Schedule 14.

ANNEX 1 TO SECTION 2: SERVICES LEVELS AND SERVICE CREDITS TABLE

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Time to Resolve The time taken to Resolve the Incident from the point of the Supplier being notified (automatically or via a report); where the root cause of such Incidents is solely due to the Supplier.	Response	Must be at least ninety-eight per cent (98%) of all Incidents within a given Service Period must be resolved within the timeframes specified within 13.6.3 of the ITT (<i>PHE ID_CIMS Further Comp_RM6068 (TePAS) Final</i>).	Not Applicable	Point five per cent (0.5%) Service Credit gained for each one per cent (1%) under the specified Service Level Performance Measure.
SaaS Uptime Uninterrupted Availability of the SaaS product where the root cause of such non-Availability is solely due to the Supplier.	Availability	Must be at least ninety-nine point five per cent (99.5%) uninterrupted Availability within the given Service Period.	Not Applicable	Point five per cent (0.5%) Service Credit gained for each one per cent (1%) under the specified Service Level Performance Measure.

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

One Service Credit has the value of one per cent (1%) of the Charges for the given Service Period; and

Service Credit Cap means six per cent (6%) of the Call Off Contract Charges for the given Service Period.

Section 3: Performance Monitoring

22. Performance Monitoring and Performance Review

- 1.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of the proposed process for monitoring and reporting of Service Levels, and the Parties will try to agree the process as soon as reasonably possible.

- 1.2 The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") as agreed pursuant to paragraph 1.1 above which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:
 - 1.2.1 for each Service Level, the actual performance achieved over the relevant Service Period;
 - 1.2.2 a summary of all failures to achieve Service Levels;
 - 1.2.3 details of any Critical Service Level Failures;
 - 1.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
 - 1.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
 - 1.2.6 such other details as the Buyer may reasonably require.
- 1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("Performance Review Meetings") on a Monthly basis to review by Performance Monitoring Reports. The Performance Review Meetings shall:
 - 1.3.1 take place within one (1) week of the Performance Monitoring Reports being issued at such location and time (within normal business hours) as the Parties may agree;
 - 1.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 1.3.3 be fully minuted by the Supplier, with the minutes circulated by to all attendees at the relevant meeting and also any other recipients agreed at the relevant meeting.
- 1.4 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

Call-Off Schedule 20 (Call-Off Specification)

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



002-INSIGHT_AND_C
ONDUEENT_PHE_ID_CI



04 Attachment 3
Public Health England



FOI Statement
(1).docx



Annex 6 - CIMS
Combined ITT Process



Annex 5 - CIMS
Scenarios for Demos



Annex 4 - Health and
Social Care Cloud Sec



Annex 3 - System
Map.pdf



Annex 2 - PHE
Security Principles.pdf



PHE
environmental_policy



Annex 7 - CIMS
Sample Data.csv

Response to Questions received on 10-May-2021

Response to queries, in red font asked on 26-May-2021, has been added in black-font and highlighted in yellow

Questions and Responses

1. Please could you review the Annex 3 - System Map (see attached) and provide evidence on how your system will integrate with PHE platforms and line of business applications as shown.

Specifically how will your system integrate with:

- AzureAD for user authentication – [Response]

Please clarify your response:

[Response]

[Redacted]

- Upstream security tooling for auditing – [Response]

[Redacted]

*Would you be able to clarify some detail on the upstream capabilities.
Can you clarify if Maven can be configured to stream logs to Azure Sentinel as per
Annex 3 – System Map?*

Please clarify your response:

[Response]

[Redacted]

- Line of business application for data exchange – [Response]

[Redacted]

[Redacted]

Can you please clarify whether Maven can integrate with our specific “Line of Business” (LOB) applications (Please refer to Annex 3 – System Map), and is also able to integrate with other applications such as Salesforce, MuleSoft, MS SQL, etc. If you could clarify if this has been done before and how much configuration will be needed or how much potential development work would be required to achieve this integration.

Please clarify your response:

[Response]

[Redacted]

If you could clarify if this has been done before and further clarify how much configuration will be need or how much potential development work would be required.

2. Please could you indicate how you follow Azure security best-practice aligned with NCSC security principles

Response

[Redacted]

[Redacted]

[Redacted]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- **Data Leakage Prevention**

Security Principle 1: PHE systems shall not have known vulnerabilities present in their infrastructure or code

Secure build and configuration standards will be adopted to ensure that systems are secure by design.

PHE systems will be specified, designed and built to ensure that commonly executed, published vulnerabilities are not present. This will include web application vulnerabilities as defined in the OWASP Top Ten.

Response

[illegible]



The image is a complex, abstract graphic design. It features a grid of black, white, and gray squares, with a blue and orange border at the top. The design is highly stylized and appears to be a digital artwork or a printmaking piece. The top border consists of a blue band with an orange line running through it. Below this, the main area is filled with a grid of squares of varying shades of gray, black, and white, creating a sense of depth and texture. The overall effect is one of a highly detailed, modern graphic.[illegible]

[REDACTED]

[REDACTED]

[REDACTED]



Security Principle 2: PHE systems will implement appropriate controls to manage offline processing of sensitive data

Where possible technical controls will be implemented to prevent the downloading of sensitive data for processing outside of system boundaries.

Where this is not possible systems will implement controls to ensure that offline processing is managed appropriately. This may include requiring staff to submit a justification for offline processing, which is logged, or restricting the devices and/or locations to which data may be downloaded.

Response



•

□

[Redacted]

[Redacted]

Security Principle 3: All access to personal confidential data on PHE ICT systems shall be attributable to individuals.

All user activity within systems containing sensitive data will be logged.

These logs will include as a minimum the name of the individual, the date and time of access and the action performed, including changes made, records viewed or queries executed.

Log information will be centrally stored and appropriately secured against tampering.

Correlation of log activity will be performed to identify and flag inappropriate or unauthorized system use. Where possible this will be used to trigger automated remediation activity.

Response

[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Security Principle 4: All access to PHE systems shall be in accordance with the principle of least privilege. Access controls will be role based.

PHE systems shall be designed so that staff are granted the minimum level of access required to enable them to carry out their duties.

Access controls will be robustly enforced and resistant to privilege escalation attempts.

As far as possible, access controls will be applied to roles or groups rather than individuals.

Response

[REDACTED]



Security Principle 5: For systems designed and built by third parties on behalf of PHE, all appropriate steps will be taken to minimize vendor lock-in.

In order that PHE has appropriate control over the security of the systems it deploys, where appropriate all intellectual property relating to systems and software shall be owned by PHE.

Where code security and intellectual property is not a consideration, open sourcing of code should be the default position.

These positions will be enforced in contractual terms with suppliers.



Security Principle 6: PHE systems holding patient data will be segregated from the wider infrastructure.

Patient identifiable information will be held on systems in secure network segments, separated from the wider data network by firewalls.

Appropriate controls will be implemented within the secure segments, and between these and the wider infrastructure. This will ensure that protection is greatest around the most sensitive assets.

Response



- [REDACTED]

At the Internet Boundary, all inbound/outbound access to Conduent networks is

[REDACTED]

Security Principle 7: PHE systems will be designed and built to support and promote interoperability

Where possible PHE will ensure that each data set held by the organisation has a single authoritative source. Where this is not possible data sets will be structured to support the efficient and reliable assembly of information from multiple systems.

PHE information systems will be structured so that data or services can be presented to other systems via common interfaces.

Response

[REDACTED]

Security Principle 8: Each staff member will be assigned a single electronic identity, which will be used for authentication to all PHE systems.

A common identity platform will be used to authenticate all access to PHE's systems.

This will enforce robust identity verification measures and will support a range of authentication options, including certificates, tokens, claims and multifactor.

Where required systems will be built to support access profiles based on user, device and location.

Response

[REDACTED]

[REDACTED]

- [illegible]