

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

Order Form

CALL-OFF REFERENCE: SR584772746/SR538127712 (Supplier Ref OPP-3292727)

THE BUYER: HM Revenue and Customs

BUYER ADDRESS 100 Parliament Street, London, SW1A 2BQ

THE SUPPLIER: Specialist Computer Centres PLC

SUPPLIER ADDRESS: [REDACTED]

REGISTRATION NUMBER: [REDACTED]

DUNS NUMBER: [REDACTED]

SID4GOV ID: [REDACTED]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 31st March 2021. It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

Lot 4 Information Assured Products & 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.

Core Terms

2. Joint Schedule 1(Definitions and Interpretation) RM6068
3. 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 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
 - Call-Off Schedules for SR584772746/SR538127712 (
 - Call-Off Schedule 5 (Pricing Details)
 - Call-Off Schedule 6 (ICT Services)
4. CCS Core Terms (version 3.0.6)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6068
6. Call-Off Schedule 4 (Call-Off Tender)
7. Annexes A to E Call-Off Schedule 6 (ICT Services)

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:

Clause 9 Core Terms – IPR ownership: Connexus UI is delivered via SaaS platform, the IPR in respect of the platform, the use of the platform, the services and data provided will remain the property of the Sub-Contractor, GB Group PLC (“GBG”) (and as appropriate GBG’s Data Suppliers & licensors). I.e. everything provided will constitute GBG’s Existing IPR for the purpose of the Core Terms and in respect of clause 9.2 no new IPR will be created which will be owned by the Buyer. GBG will not be providing Deliverables. The Call Off will also need to clarify that the Buyer will receive a licence for use of the Services for the duration of the Call Off and not a perpetual, royalty free licence. The Buyer will not be permitted to sub-licence the Services;

Clause 10.3.2 Core Terms – termination for convenience: should the Buyer terminate the Call Off for convenience, then the Buyer will remain liable to pay the Charges in respect of the 3 year term, payable up until the End Date;

Joint Schedule 11 (Processing Data), clause 6 – notification requirements: GBG can commit to notifying the Controller “without undue delay”, in line with the requirements of GDPR

Core Terms

“Force Majeure: in respect of the Services, the definition of “Force Majeure Event” contained within Joint Schedule 1(Definitions) shall take precedence over the definition of “Event of Force Majeure” as contained within the GBG Flat File Data Supply Terms and the GBG Connexus Data Services Agreement v3.0 below

GBG Flat File Data Supply Terms shall apply to this Contract. A copy of which can be found in Annex B of Call Off Schedule 6. The Connexus UI licences are provided pursuant to the terms accessible via this link - www.gbGPLC.com/gbgconnexus-dataservicesagreement-v30

The Sub-Contractor, GBG, will co-operate with the Buyer to determine whether WCAG is applicable to the Services. If it is determined to the Supplier’s reasonable satisfaction that WCAG is applicable, then within 90 days of this determination the Supplier will arrange to carry out a WCAG 2.1 AA compliance audit, undertaken by an agreed third party (which shall be subject to appropriate confidentiality obligations) to evaluate whether the Connexus Services meets the requirements of the guidelines and works with commonly used assistive technology such as JAWS screen reader, screen magnifiers and voice input tools like Dragon.

The Sub-Contractor will co-operate with the auditor regarding the findings of the audit. The Sub-Contractor will use the outcome of the compliance audit to provide the Buyer with a plan to address the findings, using reasonable endeavours, to make the adjustments identified by the 1st anniversary of the contract.

HM REVENUE & CUSTOM’S MANDATORY TERMS

- A. For the avoidance of doubt, references to ‘the Agreement’ mean the attached Call-Off Contract between the Supplier and the Authority. References to ‘the Authority’ mean ‘the Buyer’ (the Commissioners for Her Majesty’s Revenue and Customs).
- B. The Agreement incorporates the Authority’s mandatory terms set out in this Schedule.
- C. In case of any ambiguity or conflict, the Authority’s mandatory terms in this Schedule will supersede any other terms in the Agreement.

1. Definitions

“Affiliate” 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 with, that body corporate from time to time;

Core Terms

- “Authority 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, and which are:
- (i) supplied to the Supplier by or on behalf of the Authority; and/or
 - (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or
- (b) any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified;
- “Charges”** the charges for the Services as specified in the contract;
- “Connected Company”** means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;
- “Control”** the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
- “Controller”, “Processor”, “Data Subject”,** take the meaning given in the GDPR;
- “Data Protection Legislation”**
- (a) the GDPR, the Law Enforcement Directive (Directive EU 2016/680) and any applicable national implementing Laws as amended from time to time;
 - (b) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy;
 - (c) all applicable Law about the processing of personal data and privacy;
- “GDPR”** the General Data Protection Regulation (Regulation (EU) 2016/679);
- “Key Subcontractor”** any Subcontractor:
- (a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or
 - (b) with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract;
- “Law”** any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of

Core Terms

section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;

- “Personal Data”** has the meaning given in the GDPR;
- “Purchase Order Number”** the Authority’s unique number relating to the supply of the Services;
- “Services”** the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods;
- “Subcontract”** any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
- “Subcontractor”** any third party with whom:
- (a) the Supplier enters into a Subcontract; or
 - (b) a third party under (a) above enters into a Subcontract, or the servants or agents of that third party;
- “Supplier Personnel”** all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier’s obligations under the Agreement;
- “Supporting Documentation”** sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice;
- “Tax”**
- (a) all forms of tax whether direct or indirect;
 - (b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction;
 - (c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions, levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and
 - (d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above,
- in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;

Core Terms

“Tax Non-Compliance”

where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC’s “Test for Tax Non-Compliance”, as set out in Annex 1, where:

- (a) the “Economic Operator” means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and
- (b) any “Essential Subcontractor” means any Key Subcontractor;

“VAT”

value added tax as provided for in the Value Added Tax Act 1994.

2. Payment and Recovery of Sums Due

- 2.1** The Supplier shall invoice the Authority as specified in the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Supplier shall procure a Purchase Order Number from the Authority prior to the commencement of any Services and the Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number:
- 2.1.1** the Supplier does so at its own risk; and
 - 2.1.2** the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.
- 2.2** Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority from time to time via the Authority’s electronic transaction system.
- 2.3** If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Authority. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

3. Warranties

- 3.1** The Supplier represents and warrants that:
- 3.1.1** in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;
 - 3.1.2** it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and
 - 3.1.3** no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier’s assets or revenue and the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Effective Date.
- 3.2** If at any time the Supplier becomes aware that a representation or warranty given by it under Clause 3.1.1, 3.1.2 and/or 3.1.3 has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.

Core Terms

3.3 In the event that the warranty given by the Supplier pursuant to Clause 3.1.2 is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4. Promoting Tax Compliance

4.1 All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.

4.2 To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

4.3 The Supplier shall provide to the Authority the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.

4.4 If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:

4.4.1 notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and

4.4.2 promptly provide to the Authority:

(a) details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

(b) such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.

4.5 The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 4.5 shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.

4.6 Upon the Authority's request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.

4.7 If the Supplier:

4.7.1 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses 4.2, 4.4.1 and/or 4.6 this may be a material breach of the Agreement;

4.7.2 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Clause 4.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or

4.7.3 fails to provide details of steps being taken and mitigating factors pursuant to Clause 4.4.2 which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the Call-Off Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4.8 The Authority may internally share any information which it receives under Clauses 4.3 to 4.4 (inclusive) and 4.6, for the purpose of the collection and management of revenue for which the Authority is responsible.

Core Terms

5. Use of Off-shore Tax Structures

- 5.1** Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract ("**Prohibited Transactions**"). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business.
- 5.2** The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.
- 5.3** In the event of a Prohibited Transaction being entered into in breach of Clause 5.1 above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses 5.1 and 5.2, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.
- 5.4** Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses 5.2 and 5.3 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

6 Data Protection and off-shoring

- 6.1** The Processor shall, in relation to any Personal Data processed in connection with its obligations under the Agreement:
- 6.1.1** not transfer Personal Data outside of the United Kingdom unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
- (a) 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;
 - (b) the Data Subject has enforceable rights and effective legal remedies;
 - (c) 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
 - (d) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

Core Terms

6.2 Failure by the Processor to comply with the obligations set out in Clause 6.1 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

7 Commissioners for Revenue and Customs Act 2005 and related Legislation

- 7.1** The Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 ('CRCA') to maintain the confidentiality of Authority Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the aforesaid obligations may lead to a prosecution under Section 19 of CRCA.
- 7.2** The Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the Supplier's obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.
- 7.3** The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel who will have access to, or are provided with, Authority Data in writing of the obligations upon Supplier Personnel set out in Clause 7.1 above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.
- 7.4** The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at Annex 2. The Supplier shall provide a copy of each such signed declaration to the Authority upon demand.
- 7.5** In the event that the Supplier or the Supplier Personnel fail to comply with this Clause 7, the Authority reserves the right to terminate the Agreement with immediate effect pursuant to the clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

Core Terms

Annex 1

Excerpt from HMRC's "Test for Tax Non-Compliance"

Condition one (An in-scope entity or person)

1. There is a person or entity which is either: ("X")
 - 1) The Economic Operator or Essential Subcontractor (EOS)
 - 2) Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*¹;
 - 3) Any director, shareholder or other person (P) which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2. X has been engaged in one or more of the following:
 - a. Fraudulent evasion²;
 - b. Conduct caught by the General Anti-Abuse Rule³;
 - c. Conduct caught by the Halifax Abuse principle⁴;
 - d. Entered into arrangements caught by a DOTAS or VADR scheme⁵;
 - e. Conduct caught by a recognised 'anti-avoidance rule'⁶ being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not affected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

¹ <https://www.iasplus.com/en/standards/ifrs/ifrs10>

² 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

³ "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any

future legislation introduced into Parliament to counteract tax advantages arising from abusive

arrangements to avoid national insurance contributions

⁴ "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others

⁵ A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

⁶ The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

Core Terms

- f. Entered into an avoidance scheme identified by HMRC's published Spotlights list⁷;
- g. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:

- i. In respect of (a), either X:
 - 1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure⁸; or,
 - 2. Has been charged with an offence of fraudulent evasion.
- ii. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.
- iii. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.
- iv. In respect of (f) this condition is satisfied without any further steps being taken.
- v. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

1.1.1 For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

⁷ Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: <https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight>

⁸ The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

Core Terms

Annex 2 Form**CONFIDENTIALITY DECLARATION**

CONTRACT REFERENCE:

('the Agreement')

DECLARATION:

I solemnly declare that:

1. I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Authority Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.
2. I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Authority Data provided to me.

SIGNED:

FULL NAME:

POSITION:

COMPANY:

DATE OF SIGNATURE:

CALL-OFF START DATE: **31st March 2021**CALL-OFF EXPIRY DATE: **30th March 2024**CALL-OFF INITIAL PERIOD: **three (3) years**CALL-OFF OPTIONAL EXTENSION PERIOD **up to two (2) one (1) year periods**

CALL-OFF DELIVERABLES

GBG Connexus IQ web portal, flat file and bulk search facility. This covers:

Licence

101399 Special Data Extract – ConnexusIQ Flat File for use in Connect x 1

Core Terms

100969 ConnexusIQ Webservice x 50

Itemised Services

Service: GBG Connexus IQ and including ConnexusIQ Flat File

Includes the following datasets for 6000 users:

ID Number Description

100327 Connexus UI Person Linked Address

100115 Historical & Current Electoral Roll (Full)

100419 Land Registry Price Paid

100326 Multi Resident Occupants

100194 Names Database S01

100168 Names Database S07

100005 Names Database S11

100143 Names Database S14

100623 Names Database S16

200237 Names Database S19

Data - Per User

100459 Business Name Searching x 6000 users

100629 EIR Insolvency Service x 6000 users

100195 Email Addresses S01 x 6000 users

100165 Email Addresses S07 x 6000 users

100400 Email Addresses S10 x 6000 users

100006 Email Addresses S11 x 6000 users

100144 Email Addresses S14 x 6000 users

100624 Email Addresses S16 x 6000 users

200238 Email Addresses S19 x 6000 users

100620 Goneaway Flags x 6000 users

100618 National Deceased Register NDR x 6000 users

Data - Per Click

100501 AddressBase Premium 6000 Clicks per annum

100059 UK Telephone Number Database 250000 Clicks per annum

223 Users (part of the total 6000) as above PLUS Enhanced Services including:

Data - Per User

100169 Insurance Data 07 - 223 Users

101585 Insurance Data 11 - 223 Users

100622 Insurance Data 16 - 223 Users

200239 Insurance Data 19 - 223 Users

200305 Visualise - 223 Users

101361 Rental Data - 223 Users

Data - Per Click

100278 Credit Information Address Links - 10000 Clicks per annum

100337 Landline Validation - 10000 Clicks per annum

100470 Mobile Validation S2 - 10000 Clicks per annum

201176 Email Validation V2 - 10000 Clicks per annum

Core Terms

LOCATION FOR DELIVERY

As per the Purchase Order

DATES FOR DELIVERY OF THE DELIVERABLES

To be agreed between the Parties

TESTING OF DELIVERABLES

NOT USED

WARRANTY PERIOD

NOT USED

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

████████████████████

CALL-OFF CHARGES

Total three year Contract Charge = £3,175,451.01 excluding VAT

To be invoiced as follows

Year 1 to be invoiced on or around 31st March 2021 -

████████████████████

Year 2 to be invoiced on or around 31st March 2022 -

████████████████████

Year 3 to be invoiced on or around 31st March 2023-

████████████████████

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

NOT USED

PAYMENT METHOD

BACS

BUYER'S INVOICE ADDRESS:

████████████████████
████████████████████
████████████████████
████████████████████
████████████████████

[REDACTED]

BUYER'S AUTHORISED REPRESENTATIVE

Jordan Warran
Higher Sourcing Officer
Jordan.warran@hmrc.gov.uk
5W Ralli Quays
3 Stanley Street
Salford
M60 9LA

BUYER'S ENVIRONMENTAL POLICY

N/A

BUYER'S SECURITY POLICY

N/A

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]

SUPPLIER'S CONTRACT MANAGER

[REDACTED]

PROGRESS REPORT FREQUENCY

N/A

PROGRESS MEETING FREQUENCY

N/A

KEY STAFF

NOT USED

KEY SUBCONTRACTOR(S)

GB Group PLC, [REDACTED]

COMMERCIALLY SENSITIVE INFORMATION

Supplier pricing and Supplier IPR including ITT response

SERVICE CREDITS

N/A

ADDITIONAL INSURANCES

N/A

GUARANTEE

N/A

SOCIAL VALUE COMMITMENT

N/A

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:	████████████████████	Signature:	████████████████████
Name:	████████████████████	Name:	████████████████████
Role:	████████████████████	Role:	████████████████████
Date:	████████████████████	Date:	████████████████████

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.

Core Terms

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,

Core Terms

	<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;

Core Terms

"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;

Core Terms

"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"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the 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

Core Terms

	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;

Core Terms

	<p>viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and</p> <p>ix) reasonable recruitment costs, as agreed with the Buyer;</p> <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"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Data Loss Event"	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;

Core Terms

"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;

Core Terms

"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> <ul style="list-style-type: none"> a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables b) is required by the Supplier in order to provide the Deliverables; and/or c) has been or shall be generated for the purpose of providing the Deliverables;
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"DPA 2018"	The Data Protection Act 2018;

Core Terms

"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;

Core Terms

"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;

Core Terms

"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;

Core Terms

"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"	<p>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> <ul style="list-style-type: none"> i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract; or <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"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HMRC"	Her Majesty's Revenue and Customs;
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the 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;
"Impact Assessment"	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <ul style="list-style-type: none"> a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the 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; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and

Core Terms

	e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Indemnifier"	a Party from whom an indemnity is sought under this Contract;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information assurance (IA)"	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
"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>

Core Terms

	<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"	<p>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> <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>

Core Terms

	<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;

Core Terms

"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: <ul style="list-style-type: none"> 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"	<ul style="list-style-type: none"> a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; <p>but shall not include the Supplier's Existing IPR;</p>
"Occasion of Tax Non-Compliance"	<p>where:</p> <ul style="list-style-type: none"> 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: <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;

Core Terms

	<ul style="list-style-type: none"> ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;
<p>"Open Book Data"</p>	<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> <ul style="list-style-type: none"> a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables; b) operating expenditure relating to the provision of the Deliverables including an analysis showing: <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) together with a list of agreed rates against each manpower grade; iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis; f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and h) the actual Costs profile for each Service Period;

Core Terms

"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;

Core Terms

“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 <p>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;</p>
“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

Core Terms

	<p>d) the cost of implementing any measures</p> <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> <ol style="list-style-type: none"> full details of the Default that has occurred, including a root cause analysis; the actual or anticipated effect of the Default; and 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"	<p>the process set out in Clause 10.4.3 to 10.4.5 (Rectification Plan Process);</p>
"Regulations"	<p>the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);</p>
"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>

Core Terms

	<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;

Core Terms

"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

Core Terms

	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: <ul style="list-style-type: none"> 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;

Core Terms

"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.

Core Terms

"Supplier Non-Performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or c) comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of 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

Core Terms

	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 – <ul style="list-style-type: none"> (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.

Core Terms

Joint Schedule 2 (Variation Form)

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

Contract Details	
This variation is between:	[delete] as applicable: CCS / Buyer] (" CCS " " the Buyer ") And [insert] name of Supplier] (" the Supplier ")
Contract name:	[insert] name of contract to be changed] (" the Contract ")
Contract reference number:	[insert] contract reference number]
Details of Proposed Variation	
Variation initiated by:	[delete] as applicable: CCS/Buyer/Supplier]
Variation number:	[insert] variation number]
Date variation is raised:	[insert] date]
Proposed variation	
Reason for the variation:	[insert] reason]
An Impact Assessment shall be provided within:	[insert] number] days
Impact of Variation	
Likely impact of the proposed variation:	[Supplier to insert] assessment of impact]
Outcome of Variation	
Contract variation:	This Contract detailed above is varied as follows: <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 **[delete]** as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Core Terms

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

Signature

Date

Name (in Capitals)

Address

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

Signature

Date

Name (in Capitals)

Address

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

- 1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under 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:
 - 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 1.2 The Insurances shall be:
 - 1.2.1 maintained in accordance with Good Industry Practice;
 - 1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
 - 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 1.2.4 maintained for at least six (6) years after the End Date.
- 1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if you aren't insured

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

Core Terms

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

4. Evidence of insurance you must provide

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

5. Making sure you are insured to the required amount

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

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.
- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

Core Terms

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

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the 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
 - 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

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

- 1.1 In this Schedule the Parties have sought to identify the 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.
- 1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	31st March 2021	Breakdown of pricing	5 years from end date
2	31st March 2021	Supplier IPR	5 years from end date
3	31st March 2021	Tender response	5 years from end date

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	<input checked="" type="checkbox"/> Working Days	
Steps taken to prevent recurrence of Default	Steps	Timescale
	1.	[date]
	2.	[date]
	3.	[date]
	4.	[date]

Core Terms

	[...]	[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

Core Terms

(but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

- (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (c) ensure that :
- (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
- (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
- (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

Core Terms

- (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.

Core Terms

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:

Core Terms

- (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;

Core Terms

- (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

In performing its obligations under this Contract, the Supplier does not expect to process personal data for the Buyer or any other person and will only process personal data on behalf of the Buyer or any other person hereunder upon receiving a separate formal written instruction from the Buyer to the Supplier requesting the Supplier to do so. In the event that the Buyer separately instructs the service provider or third party contractors or suppliers (including any sub-contractors of the Supplier) whether verbally or in writing to process personal data or makes personal data available to them without instructing the Supplier to process that data then it engages those entities directly for those separate processing purposes and the Supplier shall not be a data processor for those separate processing arrangements.

For the Avoidance of doubt, for the purpose of the Services, GBG shall be acting as the Buyer's Processor if appointed by the Buyer separately and the Buyer shall be acting as Controller. The Supplier shall not be processing any personal data on behalf of the Buyer

Call-Off Schedule 5 (Pricing Details)

As per the Order Form

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):

- "Buyer Property"** the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
- "Buyer Software"** any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
- "Buyer System"** the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this 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;
- "Defect"** any of the following:
- a) any error, damage or defect in the manufacturing of a Deliverable; or
 - b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or
 - c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this 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

Core Terms

	whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;
"Emergency Maintenance"	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;
"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;
"Maintenance Schedule"	has the meaning given to it in paragraph 8 of this Schedule;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"New Release"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's

Core Terms

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;

"Permitted Maintenance"

has the meaning given to it in paragraph 8.2 of this Schedule;

"Quality Plans"

has the meaning given to it in paragraph 6.1 of this Schedule;

"Sites"

has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;

"Software"

Specially Written Software, COTS Software and non-COTS Supplier and third party Software;

"Software Supporting Materials"

has the meaning given to it in paragraph 9.1 of this Schedule;

"Source Code"

computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;

"Specially Written Software"

any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;

"Supplier System" the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

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

3. Buyer due diligence requirements

3.1. 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;

Core Terms

- 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;

Core Terms

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

Core Terms

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

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),

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 Licence Terms

- 10.1.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in Annex A of this Call-Off Schedule 6.
- 10.1.1.2. Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in Annex B of this Call-Off Schedule 6.

Core Terms

ANNEX A**Non-COTS Third Party Software Licensing Terms****NOT USED****ANNEX B****COTS Licensing Terms****GENERAL TERMS AND CONDITIONS**

These General Terms shall apply to the supply of Data as set out in the Order Form. Additional Terms apply as set out on the Order Form.

1 DEFINITIONS AND INTERPRETATION

1.1 In these General Terms the following definitions shall apply:

“Additional Terms” means the special terms and conditions relating to the Data sets as updated from time to time which are available at <https://www.gbtplc.com/uk/additionalterms> which will apply if the Client has selected to purchase that Data as specified on the Order Form.

“Agreement” means the Additional Terms, these General Terms, and the relevant Order Form, which in the case of conflict rank in the order of precedence set out above.

“Business Day” means Monday to Friday (excluding public and bank holidays in England).

“Charges” means the charges set out in the Order Form.

“Client” means the organisation, firm, company or public authority named on the Order Form that receives the Data provided by GBG.

“Confidential Information” means any information relating to the business of the disclosing Party which is not publicly available including, but not limited to, (i) information regarding the business, affairs, customers, clients, suppliers, operations, processes, product information, know-how, technical information, designs, trade secrets or software of the disclosing Party; (ii) any information, findings, data or analysis derived from Confidential Information including the Data; (iii) the existence and terms of this Agreement; and (iv) any other information which should otherwise be reasonably regarded as possessing a quality of confidence or as having commercial value in relation to the business of the disclosing Party.

“Contract Start Date” means the date specified as the contract start date on the Order Form.

Core Terms

“**Data**” means the data that is provided by GBG or its third party licensors as part of the provision of the Service. Any additional terms relating to the use of the Data will be detailed within the applicable Additional Terms.

“**Data Subject**” means an identifiable natural person about whom a Controller holds Personal Data. For the purposes of this Agreement, this may include an individual whose details are contained within the Data.

“**Event of Force Majeure**” means any one or more acts, events, omissions or accidents beyond the reasonable control of a Party, including but not limited to: strikes, lock-outs or other industrial disputes (other than a Party’s own); failure of a utility service, or transport network or information technology or telecommunications service; act of God (including without limitation fire, flood, earthquake, storm or other natural disaster); war, threat of war, riot, civil commotion or terrorist attack; malicious damage

(including without limitation the acts of hackers); epidemic; compliance with any law or governmental order, rule, regulation or direction; and/or default, non-performance or late performance of suppliers or sub-contractors.

“**GBG**” means GB Group plc of The Foundation, Herons Way, Chester Business Park, Chester, CH4 9GB registered in England No 2415211, including its authorised sub-contractors and agents.

“**Group Company**” means in relation to a Party, that Party, any subsidiary or holding company from time to time of the Party and any subsidiary from time to time of a holding company of that Party, as defined by s1159 of the Companies Act 2006, as amended from time to time.

“**Intellectual Property Rights**” means (i) patents, rights to inventions, rights in designs, trademarks and trade names, copyright and related rights, rights in goodwill, database rights and know-how, whether registered or not; (ii) all other intellectual property rights

or forms of protection and similar or equivalent rights anywhere in the world (whether registered or not) which currently exist or are recognised in the future; and (iii) all applications, extensions and renewals to any such rights.

“**Licence**” means the licence granted to the Client at clause 3.1.

“**Order Form**” means the order form annexed to or relating to this Agreement as accepted by the Parties.

“**Party**” means a party to this Agreement and “**Parties**” shall be construed accordingly.

“**Permitted Purpose**” means the purpose set out in clause 4.2, subject to the limitations and conditions set out in clause 4.

“**Permitted User**” means anyone who has been given access to the Data provided as part of the Service by the Client in accordance with the terms of this Agreement.

“**Personal Data**” means data which relates to a living individual who can be identified (i) from that data, or (ii) from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

Core Terms

“**Privacy and Data Protection Requirements**” means all applicable laws and regulations relating to the processing of personal data and privacy in any relevant jurisdiction, including, if relevant, the GDPR, the Data Protection Act 2018, the LED the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful

Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) and the Privacy and Electronic Communication Regulations 2003, any amendment, consolidation or re-enactment thereof, any legislation of equivalent purpose or effect enacted in the United Kingdom, and any orders, guidelines and instructions issued under any of the above by relevant national authorities, a judicial authority in England and Wales or a European Union judicial authority.

“**Service**” means the sourcing and provision of Data as a flat data file in accordance with the Client’s instructions as specified in the Order Form to the Client.

1.2 The headings in this Agreement do not affect its interpretation.

1.3 References to clauses, sections and appendices are to clauses, sections and appendices of this Agreement.

1.4 Words in the singular include the plural and vice versa.

1.5 A reference to “writing” or “written” does not include electronic mail or facsimiles

2 TERM OF THE AGREEMENT

2.1 This Agreement will start on the Contract Start Date and will continue for until the Services are completed, after which it will automatically terminate.

3 PROVISION OF THE DATA

3.1 The Client has requested that GBG act as its agent in the sourcing and acquisition of the Data and shall provide that Data to the Client in accordance with the terms of this Agreement.

3.2 Subject to the terms and conditions of this Agreement, GBG grants to the Client licence (the “**Licence**”) to use the Data for the Permitted Purpose specified in the Additional Terms.

3.3 GBG will make one copy of the Data available for the Client to download at a secure SFTP as soon as practicable following the Contract Start Date. GBG will use reasonable endeavours to provide the Data in accordance with any timetable agreed with the Client. However, the Client acknowledges and accepts that any dates given by GBG are estimates only.

3.4 If specified in the Order Form, GBG may provide suppressions / updates to the Data capturing all changes to the Data from the underlying source providers. The Client shall ensure that all suppressions / updates are applied immediately on receipt to ensure compliance with Privacy and Data Protection Requirements.

3.5 The Client must inform GBG, without undue delay, of any changes to the information which the Client supplied within the Order Form.

4 USE OF THE DATA

4.1 The Client shall comply with these General Terms and all relevant Additional Terms to this Agreement.

Core Terms

4.2 Subject to the restrictions and conditions set out within this clause 4, the Client shall be entitled to use the Data for the purposes set out in the Additional Terms only (the **“Permitted Purpose”**).

4.3 The Data is protected by Intellectual Property Rights. The Client must not copy, store, adapt, modify, transmit or distribute the Data except to Permitted Users or permit anyone else to do the same unless expressly permitted in the Additional Terms.

4.4 The Client warrants that it shall comply with all applicable legislation, instructions and guidelines issued by regulatory authorities, relevant licences and any other codes of practice which apply to the Client and its use of the Data.

4.5 The Client is responsible for the acts and omissions of all Permitted Users of the Data and is liable for any failure by a Permitted User to perform or observe the terms and conditions of this Agreement including without limitation to the provisions set out in the Additional Terms.

4.6 If the Client uses the Data in contravention of this clause 4 then GBG shall be entitled to treat the contravention as a material breach of this Agreement which cannot be remedied for the purposes of paragraph 11.2(b).

5 SECURITY

Where relevant for the provision of the Data:

5.1 The Client is responsible for the security and proper use of all user identities (**“User IDs”**) and passwords used in connection with the delivery of the Data.

5.2 The Client shall take all necessary steps to ensure that User IDs are kept confidential, secure, are used properly and are not disclosed to any unauthorised parties.

5.3 The Client must immediately inform GBG if there is any reason to believe that a User ID or password has or is likely to become known to someone not authorised to use it or is being or is likely to be used in an unauthorised way.

5.4 GBG reserves the right to suspend User ID and password access if at any time GBG reasonably considers that there is or is likely to be a breach of security or misuse of the Data.

6 CHARGES AND PAYMENT

6.1 The Client shall pay all Charges due under this Agreement within 28 days of the date of the invoice. The due date for all invoices issued by GBG shall be 28 days from the date of the invoices.

6.2 If specified in the Order Form that the Client is to pay the Charges in advance or by direct debit then such payments shall be made on or before the date specified in the Order Form.

6.3 Charges will be invoiced and paid in pounds sterling unless otherwise agreed in the Order Form. Where applicable, Value Added Tax will be added to the Charges.

6.4 If the Client fails to pay any part of the Charges when due, it shall be liable to pay GBG interest on such part of the Charges from the due date for payment at an annual rate of 8% above the base lending rate of National Westminster Bank plc from time to time accruing at a daily rate until payment is made in full in accordance with the Late

Core Terms

Payment of Commercial Debts (Interest) Act 1998.

6.5 The Client shall make all payments due under this Agreement without any deduction whether by set-off, counterclaim, discount, abatement or otherwise.

7 INTELLECTUAL PROPERTY RIGHTS

7.1 The Client acknowledges that all Intellectual Property Rights in the Service and the Data belong and shall continue to belong to GBG and/or GBG's third party suppliers.

7.2 The Client agrees not to remove, suppress or modify in any way any proprietary marking, including any trade mark or copyright notice, on or in the Data or which is visible during its operation. The Client shall incorporate such proprietary markings in any back-up copies.

7.3 The Client shall notify GBG immediately and fully co-operate with GBG to remedy the issue as soon as practicable if the Client becomes aware of any unauthorised access to, use or copying of any part of the Data by any person.

7.4 If any third party makes or threatens to make a claim against GBG, the Client or one of GBG's third party suppliers that the use of the Data or part thereof infringes any third party's Intellectual Property Rights, GBG shall be entitled to do one or more of the following:-

(a) withhold and/or request the deletion any affected element of Data that is subject to the infringement claim made by the third party;

(b) modify, replace or substitute the Data so as to avoid any alleged infringement, provided that the modification or substitution does not materially affect the quality of the Data;

(c) terminate the Agreement upon written notice to the Client and provide a refund to the Client of advanced payment made by the Client which at the date of termination has not been and will not be credited against Charges due to GBG.

7.5 The Client warrants that it will not use or exploit the Intellectual Property Rights in the Service or Data or permit others to use or exploit the Intellectual Property Rights in the Service or Data outside of the terms of the licence granted to the Client in clause 4 of this Agreement.

8 CONFIDENTIALITY AND PUBLICITY

8.1 Each Party undertakes that it shall not at any time disclose the other Party's Confidential Information to any third party except as permitted by clauses 8.3, 8.4 and 8.5 or to the extent necessary for the proper performance of this Agreement.

8.2 Each Party warrants to the other that it shall apply the same security measures and degree of care to Confidential Information disclosed to it as it takes in protecting its own Confidential Information and in any event no less than that which a reasonable person or business would take in protecting its own Confidential Information.

8.3 Neither Party shall use the other Party's Confidential Information for any purpose other than to perform its obligations under this Agreement.

8.4 Each Party may disclose the other Party's Confidential Information:

Core Terms

(a) to its or its Group Companies' employees, officers, representatives, advisers and third party suppliers who need to know such information to perform its obligations under this Agreement. Each Party shall ensure that its and its Group Companies' employees, officers, representatives, advisers and third party suppliers to whom it discloses the other Party's confidential information comply with this clause 8; and

(b) as may be required by law, court order or any governmental or regulatory authority;

For the purposes of this clause 8, Confidential Information shall not include information which:

(a) is or becomes generally available to the public (other than through a breach of this Agreement);

(b) is lawfully in the possession of the other Party before the disclosure under this Agreement took place;

(c) is obtained from a third party who is free to disclose it; or

(d) the Parties agree in writing is not confidential or may be disclosed.

9 DATA PROTECTION

9.1 Both Parties warrant that they will comply with their respective obligations under the Privacy and Data Protection Requirements.

9.2 The Parties acknowledge that for the purposes of this Agreement, the Client is the Data Controller and GBG shall source and acquire the Data on behalf of the Client as Data Processor as defined under the under the Privacy and Data Protection Requirements.

9.3 The Client warrants to GBG that it shall at all times:

(a) maintain the confidentiality and integrity of the Data received from GBG;

(b) not modify the Data or disclose or permit the disclosure of the Data to any third party unless specifically authorised to do so in writing by GBG, or required to do so by the order of a Court or a competent regulatory body;

(c) implement and maintain appropriate technical and organisational security measures against unauthorised or unlawful processing of the Data and against accidental loss or

destruction of or damage to the Data in accordance with the Privacy and Data Protection Requirements and immediately (and in any event within 48 hours of the occurrence of any breach) notify GBG of any breach or suspected breach of such security measures;

(d) not process or transfer any the Data received from GBG outside the European Economic Area without the prior written consent of GBG;

(e) co-operate with GBG to enable GBG to comply, within the timeframes required by the Privacy and Data Protection Requirements, with any exercise of rights by a Data Subject pursuant to the Privacy and Data Protection Requirements in respect of the Data pursuant to this Agreement;

Core Terms

(f) promptly notify GBG of any assessment, enquiry, notice or investigation by the UK Information Commissioner or any equivalent supervisory authority in any other jurisdiction in respect of the Personal Data supplied under this Agreement and

comply with the same including without limitation, providing all Data requested by GBG within the time scale reasonably specified by GBG in each case;

(g) take reasonable steps to ensure the reliability of all Permitted Users who have access to the Data; and

(h) where a Data Subject exercises his or her right under any laws in respect of the Data or where GBG is required to deal or comply with any assessment, enquiry, notice or investigation by any regulatory or legal body co-operate with GBG's reasonable requests to enable it to comply with its legal obligations which arise as a result of the exercise of such rights or as a result of such assessment, enquiry, notice or investigation.

10 LIABILITY

10.1 Neither Party excludes or limits its liability for death or personal injury resulting from its negligence, fraudulent misrepresentation or any other type of liability that cannot by law be excluded or limited.

10.2 Neither Party excludes or limits its liability in respect of clauses 7 (Intellectual Property Rights), 8 (Confidentiality) and 9 (Data Protection) of this Agreement.

10.3 Subject to clauses 10.1 and 10.2, each Party's aggregate liability to the other Party under or in connection with this Agreement, whether such liability arises in contract, tort (including, without limitation, negligence) misrepresentation or otherwise, shall be limited to either the Charges payable under the Agreement.

10.4 Subject to clauses 10.1 and 10.2, neither Party shall be liable for loss of profits, business or anticipated savings, loss or destruction of data, loss of use of data, loss of reputation, loss of goodwill, any special, indirect or consequential loss or damage.

10.5 The Client acknowledges and accepts that GBG has not carried out its usual due diligence process in respect of the procurement of Data in accordance with the Client's instructions. Consequently, the Client acknowledges that is solely responsible for the decision to acquire such Data and GBG cannot warrant:

(a) the accuracy, suitability for purpose/requirements and/or uninterrupted availability of the Service or Data;

(b) that the use of the Service and/or the Data will meet the Client's business requirements. Consequently, the Client agrees that the Service and the Data is

provided on an "as is" basis and except as expressly set out in this Agreement, all warranties, conditions and other terms relating to the Service, the Data and this Agreement whether express or implied by law, custom or otherwise are, to the fullest extent permitted by law, excluded from this Agreement.

10.6 The Parties acknowledge that damages alone may not be an adequate remedy for a breach by the other Party of clauses 4 (Use of the Data), 7 (Intellectual Property Rights), 8 (Confidentiality) and 9 (Data Protection) of this Agreement. Accordingly, without prejudice to any other rights and remedies it may have, the injured Party shall be entitled to seek specific performance and/or injunctive or other equitable relief.

11 SUSPENSION AND TERMINATION

11.1 GBG may suspend the provision of all or part of the Data immediately and without notice in the event that the Client breaches or GBG acting reasonably suspects that the Client has committed a material breach of any term of this Agreement.

11.2 Either Party may terminate this Agreement on immediate notice in writing to the other if any of the following applies:

(a) the other Party commits a material or persistent breach of this Agreement, which is capable of remedy, and it fails to remedy the breach within 10 Business Days of a written notice to do so. A breach shall be capable of remedy if the Party in breach

can comply with the provision in question in all respects other than as to the time of performance;

(b) the other Party commits a material or persistent breach of this Agreement which cannot be remedied;

(c) any meeting of creditors of the other Party is held or any arrangement or composition with or for the benefit of its creditors (including any voluntary arrangement as defined in the Insolvency Act 1986) is proposed or entered into by or in relation to the other Party (other than for the purpose of a bona fide solvent re-construction, re-organisation or amalgamation);

(d) the other Party ceases or threatens to cease carrying on business or is or becomes unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986; (e) a nominee, supervisor, receiver, administrator, administrative receiver or liquidator is appointed in respect of the other Party or any encumbrancer takes possession of, or any distress, lien GBG | Connexus Data Supply Agreement v4.0 (26.03.2020) execution or other process is levied or enforced (and is not discharged within seven days) upon, the assets of the other Party;

(f) an order is made for the bankruptcy or winding-up of the other Party or a resolution for its winding up is passed;

(g) a notice of intention to appoint an administrator is filed with the court or served on any creditor of the other Party;

(h) an application for an administration order is issued at court in respect of the other Party;

(i) a meeting is convened for the purpose of considering a resolution for the winding up of the other Party or the making of an application for an administration order or the dissolution of the other Party; or

(j) any event analogous to any of clauses 11.2(c) to (i) above occurs in any jurisdiction.

11.3 When this Agreement terminates the Client will:

(a) cease using the Data immediately;

(b) delete all copies of the Data in its possession within 7 days of termination and where requested by if requested by GBG provide a Data deletion certificate confirming compliance with this clause 11.3;

(c) promptly pay any outstanding and unpaid invoices due for the use of the Service and Data whether the invoice was submitted before or after the termination of this Agreement.

Core Terms

11.4 When this Agreement terminates the Parties will return or destroy (at the option and request of the disclosing Party) any Confidential Information belonging to the other Party in its possession or control other than the Data which should be deleted in accordance with clause 11.3.

11.5 The termination of this Agreement does not affect the accrued rights, remedies and obligations or liabilities of the Parties existing at termination. Nor shall it affect the continuation in force of any provision of this Agreement that is expressly or by implication intended to continue in force after termination.

11.6 If GBG terminates this Agreement during the Initial Period following a breach of this Agreement by the Client the Client agrees to pay GBG the Charges due, if any, for the remaining part of the Initial Period in accordance with clause 11.3.

12 AUDIT RIGHTS

12.1 GBG is required by its third party data suppliers and regulatory bodies to include a right of audit in all of its Client Agreements. The following provisions of this clause 12 are to give effect to that requirement.

12.2 Upon reasonable prior written notice to the Client and upon reasonable grounds, GBG shall be entitled to conduct an on-site audit or to appoint a third party auditor to conduct an on-site audit for the purposes of investigating the Client's compliance with its obligations under this Agreement.

12.3 Audits shall not be carried out on more than one occasion per year of this Agreement unless GBG reasonably believes that the Client is in material breach of the Agreement or unless GBG is required to do so by any regulatory body with competent jurisdiction or one of GBG's third party Data suppliers. GBG or its auditor may be accompanied by representatives of any such regulatory body or third party supplier in respect of any such audit imposed on GBG.

12.4 All audits will be conducted in a manner that does not materially disrupt, delay or interfere with the Client's performance of its business and shall be carried out at the expense of GBG or its third party suppliers. Should the audit reveal a breach of the Agreement by the Client, the Client shall reimburse GBG or its third party suppliers for the full cost of the audit.

12.5 The Client shall provide GBG (or any regulatory body or third party supplier as relevant) with full access to its premises, employees, computers, IT systems and records as required for the purpose of any such audit.

12.6 Prior to undertaking an audit under this clause 12 GBG shall be entitled (but not obligated) to submit to the Client questions regarding the Client's performance of its obligations under this Agreement. The Client shall respond to these questions within 14

days of receiving such request. The submission of questions under this clause 12.6 will not prejudice GBG's audit rights under this clause.

13 DISPUTE RESOLUTION

13.1 If a dispute arises out of or in connection with this Agreement or the performance, validity or enforceability of it (a "Dispute") then the Parties shall follow the procedure set out in this clause 13, specifically:

Core Terms

(a) either Party shall give to the other written notice of the Dispute, setting out its nature and full particulars (a “Dispute Notice”), together with relevant supporting documents. On service of the Dispute Notice, authorised representatives of GBG and the Client shall attempt in good faith to resolve the Dispute;

(b) if the authorised representatives of GBG and the Client are for any reason unable to resolve the Dispute within 10 Business Days of service of the Dispute Notice, the Dispute shall be escalated to senior officers of GBG and the Client who shall attempt in good faith to resolve the matter; and

(c) if the senior officers of GBG and the Client are for any reason unable to resolve the Dispute within 30 Business Days of it being referred to them, the parties will attempt to settle it by way of mediation. Should the parties fail to reach a settlement within 25 Business Days from the date of engaging in such mediation, the Parties shall be entitled to refer the Dispute to the courts of England and Wales in accordance with clause 16.2 of this Agreement.

13.2 Notwithstanding clause 13.1 above, the Parties shall be entitled to seek injunctive or other equitable relief at any point should that Party deem it necessary to protect the legitimate business interests of that Party.

14 EVENT OF FORCE MAJEURE

14.1 Neither Party shall be in breach of this Agreement nor liable for any delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure results from a Force Majeure Event. In such circumstances the affected Party shall be entitled to a reasonable extension of the time for performing such

obligations. If the period of delay or non-performance continues for three consecutive months, the Party not affected may terminate this Agreement immediately by giving written notice to the affected Party.

15 MISCELLANEOUS

15.1 The Client may not assign or transfer (in whole or part) any of its rights or obligations under this Agreement, without GBG’s prior written agreement (which must not be unreasonably withheld or delayed).

15.2 GBG will inform the Client if it assigns or transfers (in whole or part) any of its rights or obligations under this Agreement. 15.3 Save where expressly stated in the Additional Terms, a person who is not party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 or otherwise to enforce any term of this Agreement.

15.4 This Agreement constitutes the entire agreement between the Parties and replaces and supersedes all previous written or oral agreements relating to its subject matter. 15.5 The Parties agree that:

(a) neither Party has been induced to enter into this Agreement by any representation, warranty or other assurance not expressly incorporated into it; and

(b) in connection with this Agreement its only rights and remedies in relation to any representation, warranty or other assurance are for breach of contract and that all other rights and remedies are excluded, except in the case of fraud.

15.6 If any provision of this Agreement (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of this Agreement, and the validity and enforceability of the other provisions of this Agreement shall not be affected.

Core Terms

15.7 This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of this Agreement, but all counterparts shall together constitute the same Agreement. No counterpart shall be effective until each Party has executed at least one counterpart.

15.8 No failure or delay by a Party to exercise any right or remedy under this Agreement or by law shall constitute a waiver of that or any other right or remedy nor shall it preclude or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other remedy.

15.9 Unless otherwise stated herein, the rights and remedies provided under this Agreement are in addition to, and not exclusive of, any other rights or remedies provided by law.

16 GOVERNING LAW AND JURISDICTION

16.1 By entering into this Agreement, the Parties warrant that they each have the right, authority and capacity to enter into and be bound by the terms and conditions of this Agreement and that they agree to be bound by these.

16.2 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including noncontractual disputes or claims) shall be governed and construed in accordance with the laws of England and subject to clause 13 both Parties submit to the exclusive jurisdiction of the English Courts, save that GBG may elect to bring proceedings against the Client in the courts of any jurisdiction where the Client or any of the Client's property or assets may be found or located.

1) Not used

2) Not used

3) Where the Client exceeds the amount of Credits/Click or Users included annually in the search Prepayment amount, such usage will be charged at the List Prices set out above and will be invoiced monthly in arrears.

4) If GBG has agreed preferential Charges or payment terms under this Agreement or if the standard Charges or payment terms that applied on the Contract Start Date have changed during the Initial Period then unless otherwise expressly agreed in writing between the Parties, GBG's standard List Prices and payment terms will prevail in respect of the Client's continued use of the Service after the Initial Period.

5) Unless otherwise detailed in the Agreement or agreed in writing between the parties, all payments will become due upon termination of this Agreement before the end of the Initial Period.

6) Professional Services are only valid for delivery by GBG in the 12 month period to which they apply and cannot be carried over into other Periods.

7) Prepayments are only valid for use in the 12 month period to which they apply and cannot be carried over into other periods.

8) If at any time GBG is able to prove that the Charges levied do not reflect the Client's actual usage, GBG may invoice the Client for any shortfall.

Core Terms

9) Consented Email Data (if applicable). The email data contained in the product is only to be used for reference purposes and must not be used as a channel of communication to an individual. The email data can only be used for the purpose of identity management, including but not limited to, tracing of individuals, verification and/or validation of the identity of individuals for the purposes of anti-money laundering regulations, national security, crime prevention and detection, antifraud processes, asset recovery and asset reunification. For the avoidance of doubt, any information derived from our services must not be used for the purposes of marketing and/or list generation.

10) Use of Consented Telephone Numbers for Third Party Contact. Where an insurance company uses consented telephone data to contact third parties involved in an insurance claim (i.e. where the insurance company does not have a contractual

relationship with the individual), the Client must warrant that the third party has provided consent for them to be contacted by the insurance company at the scene of an accident (i.e. by providing their name and address). Where the individual has provided the incorrect name/address details, this should be referred to the police. Connexus should not be used to find the correct details. Where the customer contacts the third party by telephone and the individual expresses their wish not to be contacted in the future, then the customer should remove the individual's telephone number from their

database and only contact them in writing at the address provided. The client cannot use the data to market goods or services to the third party data subject.

Batch Capability and Connexus IQ API. 50 Users, Fair Use of 50,000 searches.

Core Terms

ANNEX C

Software Support & Maintenance Terms

NOT USED

ANNEX D

Software as a Service Terms

The Connexus UI licences are provided pursuant to the terms accessible via this link - www.gbgplc.com/gbgconnexus-dataservicesagreement-v30 **Annex E**

Device as a Service Terms

NOT USED

Core Terms

Core Terms

1. Definitions used in the contract

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

2. How the contract works

2.1 The Supplier is eligible for the award of Call-Off Contracts during the Framework Contract Period.

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

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

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

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

2.5 Each Call-Off Contract:

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

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

2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant

Authority no warranty of its accuracy is given to the Supplier.

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

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

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

2.10 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

3. What needs to be delivered

3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

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

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

3.2 Goods clauses

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

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

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

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

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

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

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

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

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

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

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

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

3.3 Services clauses

3.3.1 Late Delivery of the Services will be a Default of a Call-Off Contract.

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

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

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

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

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

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

4 Pricing and payments

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

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

4.3 All Charges and the Management Charge:

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

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

4.5 A Supplier invoice is only valid if it:

- includes all appropriate references including the Contract reference number and

other details reasonably requested by the Buyer

- includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any)
- doesn't include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge)

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

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

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

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

4.9 If CCS or the Buyer uses Clause 4.8 then the Framework Prices (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.

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

- the relevant item being made available to the Supplier if required to provide the Deliverables
- any reduction in the Framework Prices (and where applicable, the Charges) excludes any unavoidable costs that must be paid by the Supplier for the substituted item, including any licence fees or early termination charges

4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they're ordered to do so by a court.

5. The buyer's obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

- neither CCS or the Buyer can terminate a Contract under Clause 10.4.1

- the Supplier is entitled to reasonable and proven additional expenses and to relief from Delay Payments, liability and Deduction under this Contract
- the Supplier is entitled to additional time needed to make the Delivery
- the Supplier cannot suspend the ongoing supply of Deliverables

5.2 Clause 5.1 only applies if the Supplier:

- gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware
- demonstrates that the Supplier Non-Performance only happened because of the Authority Cause
- mitigated the impact of the Authority Cause

6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the End Date.

6.3 The Supplier must allow any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit.

6.4 The Supplier must provide information to the Auditor and reasonable co-operation at their request.

6.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

- tell the Relevant Authority and give reasons
- propose corrective action
- provide a deadline for completing the corrective action

6.6 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:

- the methodology of the review
- the sampling techniques applied

- details of any issues
- any remedial action taken

6.7 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

7.1 The Supplier Staff involved in the performance of each Contract must:

- be appropriately trained and qualified
- be vetted using Good Industry Practice and the Security Policy
- comply with all conduct requirements when on the Buyer's Premises

7.2 Where a Buyer decides one of the Supplier's Staff isn't suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.

7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.

7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

8.1 The Supplier warrants and represents that:

- it has full capacity and authority to enter into and to perform each Contract
- each Contract is executed by its authorised representative
- it is a legally valid and existing organisation incorporated in the place it was formed
- there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract
- it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract
- it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract
- it is not impacted by an Insolvency Event
- it will comply with each Call-Off Contract

8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.

8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:

- wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract
- non-payment by the Supplier of any tax or National Insurance

8.4 All claims indemnified under this Contract must use Clause 26.

8.5 CCS or a Buyer can terminate the Contract for breach of any warranty or indemnity where they are entitled to do so.

8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.

8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

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

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

9.2 Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.

9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:

- obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR
- replace or modify the relevant item with substitutes that don't infringe IPR without adversely affecting the functionality or performance of the Deliverables

10. Ending the contract

10.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

10.3 Ending the contract without a reason

10.3.1 CCS has the right to terminate the Framework Contract at any time without reason or liability by giving the Supplier at least 30 days' notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.3.2 Each Buyer has the right to terminate their Call-Off Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- there's a Supplier Insolvency Event
- there's a Contract Default that is not corrected in line with an accepted Rectification Plan
- the Relevant Authority rejects a Rectification Plan or the Supplier does not provide it

within 10 days of the request

- there's any material default of the Contract
- there's a Default of Clauses 2.10, 9, 14, 15, 27, 32 or Framework Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract
- there's a consistent repeated failure to meet the Performance Indicators in Framework Schedule 4 (Framework Management)
- there's a Change of Control of the Supplier which isn't pre-approved by the Relevant Authority in writing
- there's a Variation to a Contract which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes)
- if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded
- the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union (TFEU) to declare that the Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations
- the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them

10.4.2 CCS may terminate the Framework Contract if a Buyer terminates a Call-Off Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If there is a Default, the Relevant Authority can, without limiting its other rights, request that the Supplier provide a Rectification Plan.

10.4.4 When the Relevant Authority receives a requested Rectification Plan it can either:

- reject the Rectification Plan or revised Rectification Plan, giving reasons
- accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties

10.4.5 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

- must give reasonable grounds for its decision
- may request that the Supplier provides a revised Rectification Plan within 5 Working Days

10.4.6 If any of the events in 73 (1) (a) to (c) of the Regulations happen, the Relevant Authority has the right to immediately terminate the Contract and Clause 10.5.2 to 10.5.7 applies.

10.5 What happens if the contract ends

Where the Relevant Authority terminates a Contract under Clause 10.4.1 all of the following apply:

10.5.1 The Supplier is responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.

10.5.2 The Buyer's payment obligations under the terminated Contract stop immediately.

10.5.3 Accumulated rights of the Parties are not affected.

10.5.4 The Supplier must promptly delete or return the Government Data except where required to retain copies by law.

10.5.5 The Supplier must promptly return any of CCS or the Buyer's property provided under the terminated Contract.

10.5.6 The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).

10.5.7 The following Clauses survive the termination of each Contract: 3.2.10, 6, 7.2, 9, 11, 14, 15, 16, 17, 18, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.6 When the supplier can end the contract

10.6.1 The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate a Call-Off Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

10.6.2 If a Supplier terminates a Call-Off Contract under Clause 10.6.1:

- the Buyer must promptly pay all outstanding Charges incurred to the Supplier
- the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated
- Clauses 10.5.4 to 10.5.7 apply

10.7 When subcontracts can be ended

Framework Ref: RM6068
Project Version: v0.1
Model Version: v3.2

At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:

- there is a Change of Control of a Subcontractor which isn't pre-approved by the Relevant Authority in writing
- the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4
- a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority

10.8 Partially ending and suspending the contract

10.8.1 Where CCS has the right to terminate the Framework Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Call-Off Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Call-Off Contracts that have already been signed.

10.8.2 Where CCS has the right to terminate a Framework Contract it is entitled to terminate all or part of it.

10.8.3 Where the Buyer has the right to terminate a Call-Off Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

10.8.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

10.8.5 The Parties must agree any necessary Variation required by Clause 10.8 using the Variation Procedure, but the Supplier may not either:

- reject the Variation
- increase the Charges, except where the right to partial termination is under Clause 10.3

10.8.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.8.

11. How much you can be held responsible for

11.1 Each Party's total aggregate liability in each Contract Year under this Framework Contract (whether in tort, contract or otherwise) is no more than £100,000.

11.2 Each Party's total aggregate liability in each Contract Year under each Call-Off Contract (whether in tort, contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Call-Off Order Form

11.3 No Party is liable to the other for:

- any indirect Losses
- Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect)

11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

- its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors
- its liability for bribery or fraud or fraudulent misrepresentation by it or its employees
- any liability that cannot be excluded or limited by Law
- its obligation to pay the required Management Charge or Default Management Charge

11.5 In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3, 9.5, 12.2 or 14.8 or Call-Off Schedule 2 (Staff Transfer) of a Contract.

11.6 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

11.7 When calculating the Supplier's liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

- Deductions
- any items specified in Clause 11.5

11.8 If more than one Supplier is party to a Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 The Supplier indemnifies CCS and every Buyer against any costs resulting from any Default by the Supplier relating to any applicable Law to do with a Contract.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

14. Data protection

14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

- tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier
- restore the Government Data itself or using a third party

14.7 The Supplier must pay each Party's reasonable costs of complying with Clause 14.6 unless CCS or the Buyer is at fault.

14.8 The Supplier:

- must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request
- must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading
- must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice
- securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it
- indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:

- keep all Confidential Information it receives confidential and secure
- not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent, except for the purposes anticipated under the Contract
- immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

- where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure
- if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party
- if the information was given to it by a third party without obligation of

confidentiality

- if the information was in the public domain at the time of the disclosure
- if the information was independently developed without access to the Disclosing Party's Confidential Information
- to its auditors or for the purposes of regulatory requirements
- on a confidential basis, to its professional advisers on a need-to-know basis
- to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

15.4 CCS or the Buyer may disclose Confidential Information in any of the following cases:

- on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer
- on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to
- if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions
- where requested by Parliament
- under Clauses 4.7 and 16

15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

15.6 Transparency Information is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

16.2 Within the required timescales the Supplier must give CCS and each Buyer full co-operation and information needed so the Buyer can:

- publish the Transparency Information
- comply with any Freedom of Information Act (FOIA) request
- comply with any Environmental Information Regulations (EIR) request

16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority's decision, which does not need to be reasonable.

17. Invalid parts of the contract

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it's valid or enforceable.

18. No other terms apply

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

19. Other people's rights in a contract

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

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

- provides a Force Majeure Notice to the other Party
- uses all reasonable measures practical to reduce the impact of the Force Majeure Event

20.2 Either party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

20.3 Where a Party terminates under Clause 20.2:

- each party must cover its own Losses
- Clause 10.5.2 to 10.5.7 applies

21. Relationships created by the contract

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 The Supplier can not assign a Contract without the Relevant Authority's written consent.

23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Relevant Authority.

23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.

23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

- their name
- the scope of their appointment
- the duration of their appointment

24. Changing the contract

24.1 Either Party can request a Variation to a Contract which is only effective if agreed in writing and signed by both Parties

24.2 The Supplier must provide an Impact Assessment either:

- with the Variation Form, where the Supplier requests the Variation
- within the time limits included in a Variation Form requested by CCS or the Buyer

24.3 If the Variation to a Contract cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

- agree that the Contract continues without the Variation
- terminate the affected Contract, unless in the case of a Call-Off Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them
- refer the Dispute to be resolved using Clause 34 (Resolving Disputes)

24.4 CCS and the Buyer are not required to accept a Variation request made by the Supplier.

24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Framework Prices or the Charges.

24.6 If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, Framework Prices or a Contract and provide evidence:

- that the Supplier has kept costs as low as possible, including in Subcontractor costs
- of how it has affected the Supplier's costs

24.7 Any change in the Framework Prices or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

25. How to communicate about the contract

25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise

the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

25.2 Notices to CCS must be sent to the CCS Authorised Representative's address or email address in the Framework Award Form.

25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Order Form.

25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

26.2 At the Indemnifier's cost the Beneficiary must both:

- allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim
- give the Indemnifier reasonable assistance with the claim if requested

26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.

26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that doesn't damage the Beneficiary's reputation.

26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

- the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money
- the amount the Indemnifier paid the Beneficiary for the Claim

27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Contract Period:

- commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2)
- do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them

27.2 The Supplier must during the Contract Period:

- create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same
- keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request
- if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses 27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

- been investigated or prosecuted for an alleged Prohibited Act
- been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency
- received a request or demand for any undue financial or other advantage of any kind related to a Contract
- suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act

27.4 If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.4 it must specify the:

- Prohibited Act
- identity of the Party who it thinks has committed the Prohibited Act
- action it has decided to take

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

- protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise
- any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

- all applicable Law regarding health and safety
- the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer Premises that relate to the performance of a Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

31. Tax

31.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

- the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant
- other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may reasonably need

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under a Call-Off Contract, the Supplier must both:

- comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions
- indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

- the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding
- the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer
- the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements
- the Buyer may supply any information they receive from the Worker to HMRC for

revenue collection and management

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

- Law
- Clause 12.1
- Clauses 27 to 32

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

- determine the Dispute
- grant interim remedies
- grant any other provisional or protective relief

34.4 The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

34.5 The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

34.6 The Supplier cannot suspend the performance of a Contract during any Dispute.

35. Which law applies

This Contract and any issues arising out of, or connected to it, are governed by English law.

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

- 1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government.
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)
- 1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.
- 1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

- 2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:
 - 2.1.1 eliminate discrimination, harassment or victimisation of any kind; and
 - 2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

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

- 3.1 The Supplier:
 - 3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
 - 3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;
 - 3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

- 3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world.
- 3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.
- 3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;
- 3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;
- 3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;
- 3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;
- 3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

- 4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- 4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;
- 4.1.3 All workers shall be provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;
- 4.1.4 not make deductions from wages:
 - (a) as a disciplinary measure

- (b) except where permitted by law; or
 - (c) without expressed permission of the worker concerned;
- 4.1.5 record all disciplinary measures taken against Supplier Staff; and
- 4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

- 5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;
- 5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;
- 5.1.3 ensure that use of overtime used responsibly, taking into account:
 - (a) the extent;
 - (b) frequency; and
 - (c) hours worked;

by individuals and by the Supplier Staff as a whole;

- 5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.
- 5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:
- 5.3.1 this is allowed by national law;
 - 5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
appropriate safeguards are taken to protect the workers' health and safety; and
 - 5.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.
- 5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

6. Sustainability

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

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

Call-Off Schedule 4 (Call Off Tender)

2. Proposed Solution

SCC and GBG is proposing the following solutions to meet HMRC's requirement:

- GBG Connexus Flat File
- GBG Connexus IQ Web Portal
- GBG Connexus IQ Enhanced
- GBG Connexus API Batch

Each solution will be supplied to meet the requirements as follows:

1. **FLAT FILE**

Using GBG Connexus Flat File which will provide the required capability below:

- File: Specification for use in Connect, which include- Full & Edited Electoral Roll, current & 10 years Historical Data, Business Data, Postcode Grid References, Date of Birth, Address-Base Premium, Consented Telephone Numbers, Consented Email Addresses, Deceased Data, X-Ref Data Extract – the requirement is to receive a monthly update;
- Flat Files that provide Full & Edited Electoral Roll only used by KAI to be provided quarterly. Additionally, access to the enhanced data sets via the 6000 licences, that have become crucial to FIS criminal investigations and also for investigations under development in RIS.

2. **DaaS WEB PLATFORM**

Using GBG Connexus IQ Web Portal to:

The web platform must have an intuitive Graphical User Interface (GUI) to enable users to quickly access a vast array of data sources to locate, confirm and validate an individual's identity. It is not practical to list and cover every type/source of data, therefore summary is provided below. Any additional data sets pertinent to tracing of UK citizens is desirable.

Access for 6,000 users to the following data sets are required:

Data Type	Update frequency	Description
Business Data	Monthly	Data set must include a description of the business, telephone numbers, financial information. Director names, home address (where available) executive names, and disqualified Directors information.
Email addresses	Monthly	Ability to search for full/partial address. Show where an individual links to multiple emails and enables re-verse searching, so will show multiple individuals link to a single email.
Current and Historic Electoral Roll	N/A	To include 25+ years of historical data and length of residency.
Dates of Birth	Monthly	Ability to search and individual along with a confirmed with DoB
Deceased Data	Monthly	Date of death where available.
Linked Addresses		To links the same named individual to an alternative address using a matched telephone number or email address.
UK Telephone Number Database	Weekly	Data from a variety of telephone number providers (BT, Virgin, etc).

In addition, GBG will supply GBG Connexus IQ Enhanced to meet the requirement for access for 223 users (included within the 6,000) 'Enhanced' users, who are required to have an increased level of access to the specific data sets:

Data Type	Update frequency	Description
Credit Linked Addresses	Daily	Real-time lookup providing previous and forwarding addresses. Also provides links for alias names
Insurance data	Monthly	The ability to indicate whether an individual has re-quested a quote for contents, car and/or home Insurance.
Live landline and mobile validation	Covers last 24 hours for UK mobiles (including international roaming)	To ascertain whether a given number is live and connectable. For mobile telephone numbers to identify the registered network, country and current location to country level (i.e. roaming country).
Email validation		Email validation service to check that a given email conforms to a valid syntax. Validates the domain and runs a DNS check. Real-time check to assess the validity of the domain and whether the email is deliverable.

The solutions will meet the following functionality:

The DaaS web platform must have proven intuitive Graphical User Interface (GUI) to allow users to search for and display the data as follows:

- Display the names, addresses, telephone numbers and dates of birth for cohabitants of the individual being traced.
- The ability for users can export results in PDF or CSV format from the results, such as name, address and telephone number. Also, the ability to easily copy text to the 'clipboard' in one click so that other HMRC systems can be searched.
- Allow users to search at least two forenames and surnames to find cohabitants of one household.
- The ability to filter/search a results page if numerous records are returned.
- Integrated Google Maps search on individual, property and business identity pages.
- Intuitive categorisation of results to allow users to quickly assess the relevance of in-formation. For example, colour coded icons throughout the product
- • Users to be able to input/search partial data and/or search for an individual using a middle initial.
- Allows the user to input partial data and use * or ? to return results e.g. chris* to return the name Christopher, Christian, etc or Sm?th to return the surname Smith, Smyth etc.
- Displays a potential married or maiden name where it looks like an individual has married and changed their name.
- Functionality to create a search radius based on miles by matching name, date of birth, dates of residence and cohabitants.
- The ability to search within a given region using the postcode field e.g. North West.
- Allows the user to input a forename and surname, then return results for names that could be switched e.g. Craig David/David Craig.

Additionally, the ability for 'Enhanced' users to:

- Visual tool for data representation. Displays Connexus and/or customer data in a dynamic graphical interface.
- Reverse lookup - Allows the user to input a telephone number or email address and return name, address and DoB details associated with it from PII database.

3. **BATCH UPLOAD FACILITY**

Using GBG Connexus API Batch, HMRC will have the ability for specific users to perform a 'batch' lookup. For a user to upload a template file of telephone numbers and receive the results back from the datasets for the DaaS users, rather than manually entering individual numbers one by one to look up and extract the results.

3. Accessibility evidence questionnaire

3.1 Background

All digital services and products purchased or run by HMRC must meet [public sector accessibility regulations](#). The regulations state that the product or service being delivered through a web browser or mobile applications must be [WCAG 2.1 AA](#) compliant.

HMRC will be breaking the law if a product purchased, developed or is in control of is not accessible.

This questionnaire should be answered in relation to any product(s) or service(s) you intend to provide through a web browser or mobile application, that will be used as part of any contract resulting from this procurement exercise.

The answers you provide will be reviewed by the HMRC accessibility team.

1. Name of bidding organisation

Specialist Computer Centres PLC on behalf of GB Group Plc

2. Does the product or service fully meet WCAG 2.1 AA?

If the answer is 'Yes', Provide evidence of how the product or service meets the standard. Evidence could include accessibility audit reports, voluntary product accessibility templates (VPAT), and accessibility statements.

If the answer is 'No', provide details of where WCAG 2.1 AA is currently partially or not met. Please also include a roadmap of how the product or service will be fully compliant by the contract operational date.

No. The flat file and batch capability are not interactive products (flat file is raw data on a disk or, as per the batch capability, received via sFTP), and as such do not have specific features to meet the WCAG standards.

Connexus IQ is provided via a web portal and as such it is the browser which is the primary contact point for the user. There is no reason why Browser plug-ins such as "Dragon" cannot be used with Connexus, and similarly features such as Browser zoom functions. Connexus IQ provides both colour and black coded icons to signify the results of a search. For any individual who is colour blind, hovering over the icon will provide information as to its meaning.

GBG is currently engaged at reviewing the accessibility of all of its products as part of its Inclusion and Diversity programme and will be producing a roadmap of potential improvements following the discovery stage of the project.

3. Has the product or service been tested with assistive technology?

If the answer is 'Yes', please provide details of which [assistive technology](#) it has been tested with.

No.

4. Describe how the product or service will remain fully WCAG 2.1 compliant during the life of the contract.

As outlined in question2, Connexus IQ will remain compliant because it is accessed via a web portal provided there are no fundamental changes to the functionality of the web browsers in use.

3.2 Additional comments

Use this space to tell us anything else that supports the evidence of the accessibility of your product or service.

3.3

3.4 Accessibility charter

HMRC has signed up to the [Accessible Technology Charter](#), created by the [Technology Taskforce](#) of the [Business Disability Forum](#). Please consider joining HMRC and other partners by signing up.



HM Revenue
& Customs

Security Plan Questionnaire (High)

To:	GB Group Plc (GBG)
From:	Jordan Warran
Date:	11/03/2021
Tender reference:	SR584772746
Tender title:	Bulk and Enhanced UK Citizen Data

Schedule 2.4 Security Plan

Background

The Contractor is required to prepare a Security Plan in accordance with the HMRC's Security Policy. The requirements set out in this Security Plan also apply to any sub-contractors engaged by the Contractor to perform any of the services under the Contract. HMRC has developed a standard set of questions and recommendations (see attached Appendices) to ensure consistency across relevant contracts. The Contractor is required to provide answers to the standard set of questions contained within this questionnaire to formulate the initial Security Plan. This Security Questionnaire covers the principles of protective security to be applied in delivering the services in accordance with HMRC's Security Policy and Standards. The Contractor's response to this questionnaire, with any subsequent amendments as may be agreed as part of a clarification process, will be included in the signed version of any resulting agreement, as confirmation that the content of the Security Plan has been agreed with HMRC.

1 Policy & Standards

1a Please confirm that you understand that your responses to this questionnaire will form the initial Security Plan and will be included in the final signed version of any resulting agreement.

Response: Confirmed

<p>1b Please confirm your organisation and any subcontractors' will conform to the requirements set out in the Government Security Policy Framework (SPF), available from Security Policy Framework and any Security Requirements recorded in the schedules and/or Order Form.</p> <p>Response: Confirmed</p>
<p>1c If you believe that the Public Sector Network (PSN) Code of Connection, available from www.gov.uk, will apply to your organisation and any sub-contractors, please provide details of how you will conform to this.</p> <p>Response: Not Applicable</p>
<p>1d Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the UK General Data Protection Regulation see UK GDPR and in accordance with Clause 23 (<i>Protection of Personal Data</i>) of the Contract.</p> <p>Response: Confirmed</p>
<p>1e Please confirm that you have paid the Data Protection Fee to the ICO or that you fall into one of the exempt categories. More information can be found here</p> <p>Response: Confirmed</p>
<p>1f Please provide details of any security accreditation that your organisation currently possesses, such as but non exclusive to, ISO 27001 and PCI DSS and describe the process used to achieve the accreditation.</p> <p>Response:</p> <p>GBG is accredited to ISO27001 and Cyber Essentials. GBG uses the services of BSI as its accreditation body who carry out annual surveillance visits to audit the processes and controls in place, with a full recertification every 3 years.</p>
<p>1g If you intend to involve sub-contractors at any stage during the Contract please list them and provide details of how you will ensure their compliance with all aspects of this Security Plan.</p> <p>Response: Not Applicable</p>

1h As appended to this Schedule 2.4, Appendix G, Security Aspects Record, defines the Government Security Classifications (see [Government Security Classifications](#)) carried by the HMRC data. If you are successful in the tender process, you will require a Security Manager (or appointed person), to take responsibility for the security of the data.

Please provide the name of your Security Manager who will act as a first point of contact and conduct ongoing management of security risks and incidents (including identification, managing, and reporting in line with agreed procedures for actual or suspected security breaches).

Response:

██████████ is GBG's Information Security Governance and Risk Manager who is responsible for managing the risks associated with GBG's Information Security Policy and Procedures to ensure that all data is secure.

2 Physical Security (For requirements please see Appendix A – Physical Security)

2a For the locations where HMRC assets are held please provide details of any procedures and security in place designed to control access to the site perimeter.

Detail measures such as fencing, CCTV, guarding, and procedures and controls in place to handle staff and visitors requesting access to the site. Please also provide details of the maintenance schedule of your security controls.

Response:

Not Applicable because no HMRC assets will be held by GBG.

2b Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas within the premises holding HMRC assets.

Detail measures such as building construction type, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Please also include details of any automated access controls, alarms and CCTV coverage.

Please also provide details of the maintenance schedule of these security controls.

Response:

Connexus Web Portal: this is hosted by Amazon Web Services at its UK (London) data centre which has the following:

Physical access is controlled at building ingress points by professional security staff utilising surveillance, detection systems, and other electronic means. Authorised staff utilise multi-factor authentication mechanisms to access data centres. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open. Physical access points to server rooms are recorded by CCTV.

Connexus API (Bulk): this is operated from GBG's data centre at its head office which has the following:

The datacentre has key card access that is limited to authorised personnel, CCTV is in place and all perimeters under control with alarms and motion detection.

3 IT Security (For requirements please see Appendix B – IT Security)

3a Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed or provide details of any cyber essentials accreditation that you are planning in the future.

Response:

GBG is accredited to Cyber Essentials.

3b Please provide details of the controls and processes you have in place covering patching, malware (anti-virus), boundary/network security (intruder detection), content checking/blocking (filters), lockdown (prevention), and how regularly you update them.

Response:

Patching: on AWS all ingress and egress traffic passes through a pair of resilient UTM (SPI) firewalls from one of the top 5 security appliance manufacturers. The devices are based on a vendor supplied hardened template, with patches applied monthly.

For Connexus all patches are applied first to the development site and tested before they are deployed to the primary site.

Malware: on GBG's own servers, Symantec anti-virus / malware software is installed on all servers. For AWS all servers are built using the default Amazon AMI images which are based on a minimal OS installation by default. Services are in place to ensure build compliance to our Info Sec standards, where toolsets such as Anti-Virus, File Integrity Monitoring and Domain Membership are installed at boot.

Intruder Detection: IDS is enabled on Firewalls. Network Intrusion Detection/Prevention rules and logs are reviewed on a regular basis by GBG's SOC team.

3c Please provide details of the overall security and access control policy of your systems covering physical and electronic assets (including communications connection equipment, e.g. bridge, routers, patch panels). You should record details of the formal registration/deregistration process, how users are Authorised, Authenticated and held Accountable for their actions. Also include details of the measures in place to manage privilege access e.g. System Administrators and remote users.

Response:

Access to GBG's systems is in accordance with GBG's Access Control Policy, with access granted on a needs basis. All systems use two-factor authentication and when working remotely it is via VPN. Physical access to GBG's offices is via swipe card access that is in line with the Starters, Movers and Leavers Policy.

All new starters are given a username and temporary password, which they must change on first sign-on. All passwords must be changed every 90 days and cannot be the same as any of the previous twelve. When an employee leaves, access rights are removed and equipment returned on the date of leaving.

An employee's contract of employment includes clauses on data protection, confidentiality and information security and that signing the contract the employee is held liable for any breach of these clauses that may result in disciplinary action.

3d Please provide details of how your security and access control policy complies with the Security Policy Framework (including where necessary, use and control of backup systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets).

Response:

Access to any GBG system is in accordance with GBG's Access Control Policy. GBG operates a role-based access/least privilege access policy. Any changes to access rights must be requested through Information Security/IT services to be approved, with user IDs and access rights reviewed regularly. Before gaining access to Connexus a page is displayed, where the user must accept that they have permitted purposes to access the product.

All ingress and egress traffic passes through a pair of resilient UTM (SPI) firewalls from one of the top 5 security appliance manufacturers. The databases are logically separated from the DMZ by firewall and routing rules, additionally each database service is contained within its own security group and accessible only by relevant services.

3e Please describe how you ensure all software and data is approved before being installed, and how your information systems are reviewed for compliance with security implementation standards (e.g. penetration testing).

Response:

All GBG systems are restricted to the software that can be deployed and only registered software can be installed. Installation of any software is either through the IT Services, Infrastructure or Info Sec teams depending on the system. Employees can only install software through the authorised Software Centre process.

GBG conduct penetration tests based on the information provided to us via our threat intelligence feeds. As and when these feeds indicate a heightened threat level against our products and assets a penetration test may be conducted with vulnerabilities remediated in a timely manner. Also, penetration tests are triggered after any major product release.

3f Please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place for the use of portable media and storage devices exceptionally loaded with HMRC data.

Response:

All laptops and desktops are locked so that portable devices e.g. USB sticks cannot be used to download anything from GBG's network. GBG uses Bitlocker to encrypt all workstation hard drives. No GBG device will access any of HMRC's data.

3g Please provide details of how all equipment (e.g. hardware, portable media) that holds or has held data will be destroyed or decommissioned, and how all data will be rendered unreadable and irretrievable in line with HMG Security Policy Framework requirements for information management.

Response:

No GBG's device will access any of HMRC's data. However, all IT equipment undergo a sanitisation process prior to disposal or reuse. Care is taken to ensure that sensitive information is deleted from equipment when it is released from business units or IT Services. All equipment is disposed of in compliance with GBG Data & Equipment Destruction Policy to ensure:

- Information storage areas of hard disks or other storage media must be erased by a secure deletion method.
- Configuration information held as part of the system or application software must be reset.
- Security software, cryptographic keys or other control elements must be securely removed.

A secure deletion method wipes the physical area of storage irreversibly rather than simply removing the disk directory reference to that information.

4 Personnel Security (For requirements please see Appendix C – Personnel Security)

4a What security vetting has been carried out for staff who will have access to, or come in to contact with HMRC data or assets.

Response:

None of GBG's employees will have access to or come in contact with HMRC's data. However, all employee candidates (regardless of permanent, temporary or contract) are screened to check:

- The applicant's identity, comprising Name, Date of Birth, driving licence and address history.
- Right to work in the UK, original passport, or full birth certificate/Visa.
- DBS and Credit Check (if relevant).
- Curriculum Vitae – 2 years' worth of references i.e. Employment History & Qualifications checks.
- Employment/Character reference checks.
- Where appropriate, financial background checks.

4b Please provide details of how you will ensure that all staff accessing HMRC data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract.

Response:

None of GBG's employees will have access to HMRC's data.

4c All contractor's personnel who have access to HMRC data, and/or are directly involved in the service provision must sign a copy of HMRC's Confidentiality Agreement. Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the CA for all personnel involved in this Contract if requested.

Response:

No GBG employees do have access to any customer data, and there is no data stored within the platform. An overarching NDA is in place between GBG and HMRC which has the effect of protecting the confidentiality of both parties' confidential information.

4d Please provide details of the ongoing training you provide to staff in respect of data security, including risk awareness and the identification and reporting of security incidents. Please also provide details of your documented information security procedures and processes that are available to all staff who will have access to, or come into contact with HMRC data.

Response:

The Information Security policy and several other policies form part of GBG's Information Security Management System (ISMS) which is the basis of GBG's accreditation to ISO27001. It is a mandatory requirement that annually all employees must undergo awareness training, that covers both the policies of the ISMS and Data Privacy. The training is a series of modules and the end of which a series of questions are asked to test the individual's understanding of the module.

In addition, following the annual review of all policies or following a major update/change, each employee is reviewed to read/review the policy and to sign to say it has been completed. This detail is recorded on the employee's personnel record.

All policies are also available to all team members via GBG's Intranet.

4e Please provide details of your procedures for on and off boarding staff.

Response:

Onboarding: Following the acceptance by the potential employee, HR will initiate the workflow as per the Starters, Movers & Leavers policy to notify IT Services and Facilities of the starting date so that the necessary equipment can be ordered and access passes arranged. The employee will be provided with a contract for signing and on the date of arrival will be given the necessary swipe card and equipment with the necessary access rights including user account and type of account, depending upon the role.

Offboarding: Business units and line managers are to inform HR immediately to notify of any future terminations, and where appropriate the circumstances of termination. As per instructions in the Starters and Leavers Policy a workflow is initiated from HR to instigate the “leavers” process. IT Services and Facilities are informed and carry out actions, as appropriate in line with policy, this will include disabling the user accounts on the day of departing. The employee is also required to return all company assets, e.g. laptop, mobile phone to their line manager or department as instructed.

5 Process Security (For requirements please see Appendix D – Process Security)

5a Please provide details of the format in which HMRC data will be held, how you will ensure segregation of HMRC data, and the locations where this data will be processed.

Response:

Not Applicable, because no data will be held.

5b Please confirm your understanding and agreement that the transfer of any HMRC asset to third parties (any individual or group other than the main Contractor) is prohibited without prior written consent from HMRC. If you anticipate transferring data, especially using portable media during the delivery of this project, please set out your proposed transfer procedures for consideration.

Response:

Confirmed but no data will be transferred to any third party.

5c Please confirm that you understand that HMRC data must not be processed or stored outside the United Kingdom without the express permission of HMRC.

If you are considering storing data outside of the UK, please provide details on how and where the data will be stored.

Please note: In line with HMRC's policies in response to current regulatory guidance, the successful supplier(s) will not be permitted to transfer any Personal Data (as defined in the UK General Data Protection Regulation (UK GDPR)) provided by HMRC in connection with any contract resulting from this procurement exercise, to the United States of America.

On this basis, HMRC reserves the right to reject a bidders entire tender submission and/or terminate any contract awarded, where it becomes apparent to HMRC that the supplier is transferring/is proposing to transfer Personal Data to the United States of America.

Response:

Confirmed, the Connexus platform is in the UK, but with DR in Ireland.

5d In order to protect against loss, destruction, damage, alteration or disclosure of HMRC data, and to ensure it is not stored, copied or generated except as necessary and authorised, please provide details of the technical and organisational measures you have in place (including segregation of duties and areas of responsibility) to protect against accident or malicious intent.

Response:

GBG's systems are fully secure in accordance with our ISO27001 accreditation and GDPR, but no HMRC data will be stored within the platform.

5e What arrangements are in place for secure disposal of HMRC assets that may be in your possession once no longer required?

Response:

Not applicable because GBG will not be holding any of HMRC's assets.

5f How and when will you advise HMRC of security incidents that impact HMRC assets that may be in your possession?

Response:

As per Article 33 of GDPR, GBG would notify the controller without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the customer data transmitted, stored or otherwise processed.

5g Please describe your disciplinary procedures in the event of a security breach involving HMRC data.

Response:

Not Applicable because no HMRC data will be stored within the platform.

5h Do you have a List X accreditation?

If 'yes', please answer the following:

- What is the name of your Security Controller?
- What/Where does the List X accreditation cover?
- For what purpose?
- Please provide evidence the Department who sponsored the List X accreditation has agreed to share the environment.

Response: No.

6 Business Continuity

6a Please provide an overview of your organisation's Business Continuity and disaster recovery plans in terms of the HMRC data under the Contract, or attach a copy of your Business Continuity Plan. Please specify if you operate Business Continuity or disaster recovery from outside the UK. Also, please provide details on when and how frequently these plans are tested and advise when they were last tested and confirm results of testing exercises are available for review if requested.

Please provide details on how you will meet recovery times if these have been specified in the schedules and/or Order Form.

Response:

GBG has in place a Business Continuity Management System (BCMS) which is aligned to ISO22301, although GBG are yet to achieve this certification.

The Business Continuity Management System document suite, or overall business continuity plans, shall be formed of:

- Business Continuity Management System Policy
- Disaster Recovery Plans
- Office Contingency Plans

GBG also has in place an Incident Management Plan which details GBG's approach and response to Incident Management at the strategic, tactical and operational level. This plan also forms part of our overall response to events, incidents and crises that may impact GBG's products and services.

For Connexus, GBG operates a dual site arrangement with AWS whereby the DR facility is located at AWS in Ireland. The platform has an active configuration split over two availability zones. Recovery time is instantaneous with no expected data loss. Should we lose an availability Zone, the secondary zone will continue to provide the service.

7 Cryptography

7a Please provide details of processes and procedures in place for handling Government cryptographic material.

Response:

Not Applicable because the searches/data to be provided should not be encrypted.

The following appendices provide additional information on the types of security control that may be expected as a minimum for the protection of HMRC information, data and assets.

It is not a legally binding document, nor does it provide a definitive list of baseline security controls. It should be read in conjunction with HMG and HMRC Security Policy and Standards.

Appendix A – Physical Security

Please consider: the effect of topographic features and landscaping on perimeter security; the possibility of being overlooked; the ease of access and communications; the existence and proximity of public rights of way and neighbouring buildings; the existence of emergency and evacuation routes from adjacent buildings; the implications of shared accommodation; the location of police and emergency services; the build of the structure.

Building Security - There should be as few points of exit and entry as possible but in line with Health & Safety and Fire Regulations. Where exit and entry points exist then physical security controls, such as window bars, grilles shutters Security Doors etc may be installed. The effectiveness of these protection measures may be enhanced by the use of Intruder Detection Systems (IDS), CCTV or Guard Service.

Physical Security	Requirements	Recommended
Secure Rooms	Construction in line with CPNI guidance; locked during 'silent hours' and keys/combinations secured. Sufficient CPNI-Approved lockable storage for material at OFFICIAL or above. Intruder alarm with key holder response.	Intruder alarm with police response. Appropriate automated access control system.
Perimeter Security		CCTV Coverage to identify intruders with adequate lighting for night-time operation. Use of fencing that offers a degree of resistance to climbing and to deter an opportunist e.g. anti-intruder fencing. Manned guarding to be considered.
Physical Access - secure areas	Visitors limited to those with a business need, issued with identifying badges upon arrival and escorted at all times.	A visitor log maintained and visitors sign in and out.

Physical Security	Requirements	Recommended
Building	<p>Constructed of robust building materials typically, brick or lightweight block walls.</p> <p>External doors of solid construction, locked during silent hours and linked to intruder detection system.</p> <p>Access to keys must be checked and any lock combinations changed at regular intervals not exceeding 12 months. A record of key/combination holders must be maintained.</p> <p>The number of keys to a lock must be kept to a minimum. Spare keys must not be held in the same container as 'working keys'.</p> <p>The premises must be locked during 'silent hours' and keys secured.</p> <p>Intruder alarm with key holder response.</p> <p>Windows double glazed or similar unit with locks.</p> <p>Emergency exit doors included on intruder detection system.</p>	<p>Security Keys should not be removed from the premises.</p> <p>Intruder alarm with police response.</p> <p>Power outage alarm with key holder response.</p> <p>Appropriate automated access control system.</p>
Environmental	<p>Fire risk assessment must be carried out.</p> <p>Uninterruptible power supply for security and health & safety equipment.</p>	<p>Smoke detection system e.g. VESDA.</p>
Transport and Storage	<p>Appropriate CPNI-Approved lockable storage for HMRC material.</p> <p>Point to point transfer of all HMRC material using CPNI-Approved locked containers and (where necessary) solid sided vehicles.</p>	<p>HMRC "trusted hand" using named individuals.</p>

Appendix B – IT Security

IT Security	Requirements	Recommended
Cyber Essentials	<p>It is mandatory for HMG suppliers to demonstrate that they meet the technical requirements prescribed by Cyber Essentials.</p>	<p>Cyber Essentials Plus with independent assessment and certification.</p>

IT Security	Requirements	Recommended
Authorisation	Users and Administrators must be authorised to use the System/Service. Higher privilege access accounts should be tightly controlled and only assigned to authorised individuals.	
Authentication ⁹	Individual passwords must be used to maintain accountability; Robust passwords should be used, that are designed to resist machine based attacks as well as more basic guessing attacks. Passwords must be stored in an encrypted form using a one-way hashing algorithm. Passwords must be able to be changed by the end user, if there is suspicion of compromise. Passwords must be changed at least every 3 months.	Machine-generated passwords. Multi-factor authentication should be considered for exposed environments and remote access. Passwords for privileged accounts/users (Administrators) etc. should be changed more frequently than every 3 months.
Access Control	User access rights to HMRC information assets must be revoked on termination of employment. Audit logs for access management in place showing a minimum of 30 days of activity.	

⁹ Authentication is the process by which people “prove” to the system that they are the person they claim to be. There are three possible authentication factors: Passwords (something a person knows), tokens (something a person possesses), and biometrics (something a person inherently is or how they behave).

IT Security	Requirements	Recommended
Malware Protection ¹⁰	<p>Malware protection software should be installed on all computers connected or able to connect to the Internet. It must be regularly updated in line with vendor recommendations or at least daily and should be configured to scan files on access and perform regular scans of all files at server and desktop level (PC/Laptop etc). It should also be configured to identify and block access to known malicious websites. Security Operating Procedures (SyOps) must ensure that malware protection is kept up to date. Anti-Virus Administrators and users should be trained on use of AV software.</p> <p>Users should receive awareness training so that they are aware of risks posed by malicious code from the use of email and attachments, internet and removable media (CD, DVD, USB devices etc).</p> <p>All users, systems and services must be provided on a least privilege basis to reduce the potential for accidental introduction of malicious code.</p> <p>For systems attaching to HMRC network, dual layered malware protection and detection capability.</p>	<p>Consideration should be given to allowing privilege users (System Administrators) to only use a limited 'non-privilege role' to conduct vulnerable operations such as browsing or importing via removable media.</p> <p>Dual layered malware protection and detection capability.</p> <p>Malware protection software should be configured to update automatically or update through the use of a centrally managed deployment. Systems and services holding assets with a Government Security Classification of Secret are expected to be air-gapped and will therefore require malware protection to be configured manually.</p>

¹⁰ CESG Good Practice Guide No 7 provides information on the threats and vulnerabilities and risks associated with malicious code and also provides guidance on appropriate risk management measures.

IT Security	Requirements	Recommended
Network Security	<p>Information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.</p> <p>Boundary controls should have content checking and a blocking policy in place e.g. firewalls. As a minimum the default administrative password for network devices such as Firewalls should be changed to a strong password comprising of a minimum of 8 characters. All unnecessary services should be disabled/'blocked' by default at the boundary firewall. It is important that Firewall rules that are no longer required are disabled/removed timeously, for example when a service is no longer required.</p> <p>The administrative interface used to manage boundary firewall configuration routinely must NOT be accessible from the Internet.¹¹</p>	<p>Dual paired firewalls, different vendors.</p> <p>Anomaly detection capability e.g. Network intruder detection system.</p>
Patch Management	<p>Software should be patched and devices, systems, operating systems and applications should be 'locked down' to remove unnecessary services and functionality. File types should be limited.</p> <p>All Critical security patches should be deployed timeously and in line with vendor recommendations. The deployment of Important i.e. less critical patches should be deployed on the basis of risk.</p>	
System Documentation	<p>System designs/architectural blue prints and network designs should be protected from unauthorised access, loss and destruction.</p>	

¹¹ It is envisaged that systems holding Secret assets will not be supported by a remote administrative and will not be Internet facing.

IT Security	Requirements	Recommended
Disposal of media	HMRC information assets must be sanitised in line with HMG IA Infosec Standard 5 Secure Sanitisation. Your CESG contact can provide further information.	
Technical Testing	IT health check aka penetration testing for front facing internet services delivered to HMRC.	Consideration for regular IT health check of application and infrastructure services delivered to HMRC.
Use of Laptops and removable recordable media.	Laptops holding any information supplied or generated as a consequence of a Contract with HMRC must have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed. Approval from HMRC must be obtained before information assets are placed on removable media ¹² . This approval must be documented sufficiently to establish an audit trail of responsibility. All removable media containing information assets must be encrypted. The level of encryption to be applied is determined by the highest HM Government Security Classification of an individual record on the removable media. Unencrypted media containing HMRC information assets must not be taken outside secure locations; the use of unencrypted media to store HMRC information assets must be approved by HMRC.	

Appendix C – Personnel Security

Personnel Security	Requirements	Recommended
Security Clearance	Pre-employment checks should meet the Baseline Personnel Security Standard (BPSS) and must be completed for all staff with potential or actual access to HMRC assets.	See www.gov.uk specifically the link to the Disclosure & Barring Service for more information.

¹² The term drives includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media and external hard drives.

Personnel Security	Requirements	Recommended
	Security Clearance for all staff with access or potential access to material with a Government Security Classification of SECRET.	Staff with privileged system access (system administrators) to have Developed Vetting Clearance.
Confidentiality Agreements	Confidentiality Agreements (CA) must be completed by all staff with potential or actual access to HMRC information assets as requested.	
Security Awareness Training	All staff must undergo security awareness training and be familiar with HMRC security policy, standards and guidance. There must be a plan in place, endorsed and owned by a named individual at Board Level, to ensure refresher training takes place at least annually.	Board members and senior management should be able to demonstrate their commitment to security through a variety of mechanisms.
Joiners and leavers	Process to ensure individuals are appointed to clearly defined roles with appropriate access rights only. Leavers' access rights to systems and premises are removed on termination of employment.	

Appendix D – Process Security

Process Security	Requirements	Recommended
Disciplinary Process	There must be an organisational disciplinary process. Staff must be briefed on this and the penalties that may result from failure to comply with documented security policies	
Security Policies, Processes and Procedures	Where the contract requires you to hold HMRC assets at Secret or above you MUST ensure there is a relationship at senior management level between your organisation and CESC. Procedures in place to determine whether any compromise of HMRC assets e.g. loss or modification of information, software and hardware has occurred.	Obtain the services of a CLAS consultant to help you through the bidding process and, if successful, the early stages of contract award.

Process Security	Requirements	Recommended
	<p>Procedures for the handling and storage of HMRC information assets must be established to protect from unauthorised disclosure and/or misuse. End of day procedures must ensure that HMRC assets are adequately protected from unauthorised access.</p> <p>A clear desk policy must be enforced.</p> <p>Procedures must be in place to ensure HMRC's assets are segregated from any other Client's assets held by the contractor.</p> <p>Procedures for the secure disposal of the HMRC's assets must be in place. Where HMRC assets are held at SECRET all staff and visitors must visibly wear an identifying pass while on site.</p> <p>Where HMRC assets are held at SECRET portable media devices must be excluded from the secure area.</p> <p>A challenge culture must be fostered, so that staff or visitors not wearing a pass are challenged. Where an access control system is in operation tailgating must be discouraged.</p> <p>Where required HMRC assets must be destroyed in line with the Security Policy Framework. Further guidance on storage and destruction of media is available from CESG.</p>	
Transfer of HMRC Data	<p>Any proposed transfer of HMRC data must be approved by HMRC in writing. If the Contractor is unsure whether approval has been given, the data transfer must not proceed.</p> <p>Where data transfers are necessary in the performance of the Contract, they should be made by automated electronic secure transmission via the Government Secure Internet (GSI) with the appropriate level of security control. Individual data records (unless as part of a bulk transfer of an anonymised respondent survey data) will require specific transfer arrangements. Transfer of aggregated data such as results, presentations, draft and final reports may also need discussion and agreement, again in advance of any such transfer.</p>	<p>Whenever possible, putting data on to removable media should be avoided. Where this is unavoidable, hard drives and personal digital assistants, CD-ROM/DVD/floppy/USB sticks are only to be used after discussion and agreement with HMRC in advance of any such transfer.</p> <p>If the use of removable media is approved, data must be written to them in a secure, centralised environment and be encrypted to HMRC's standards.</p>

Process Security	Requirements	Recommended
		If you anticipate transferring data on removable media during the delivery of this project please set out your proposed transfer procedures.
Incident Management	Arrangements must be in place for reporting security breaches to the asset owner.	
List X	<p>Further information on List X is available at www.gov.uk.</p> <p>A List X accreditation may just cover a floor, a room or even a particular piece of secure furniture and may be for a specific purpose.</p> <p>Note: If you do have a List X accreditation, please keep responses generalised for the purposes of completion of this question.</p>	

Appendix E – Business Continuity

Business Continuity Requirements	Requirements	Recommended
Business Continuity Management	3 rd party suppliers should provide HMRC with clear evidence of the effectiveness of its Business Continuity management arrangements and alignment with recognised industry standards, by assessing risks to their operations and producing and maintaining business continuity documentation.	

Appendix F – Cryptography

Government Cryptography	Requirements	Recommended
Cryptographic Material	Information on this subject will be available from your contact in CESG.	

Schedule 2.4 – Appendix G – Security Aspects Record

- G.1. This contract will involve the Contractor holding UK Government security classified material (*replace “security classified” with “classified” for overseas companies*). It is a condition of this contract that this material must be protected. The standard of protection required is detailed below and varies with the level of security classification. Material passed to the Contractor will bear the security classification appropriate to it.
- G.2 In determining the Security Classification ‘Aggregated Material’ has been considered. ‘Aggregation’ is the term used to describe the situation when a large number of data items at one classification are collected together. The impact of the compromise of the whole collection can often be significantly higher than the Impact of compromise of one item. This applies to compromises of Confidentiality, Integrity and Availability.
- G. 3 To assist the Contractor in allocating any necessary classification to material which the Contractor may produce during the course of the contract and thus enable the Contractor to provide the appropriate degree of protection to it, this schedule formally advises you of the correct security classification to apply to the various aspects of the contract.
- G.4 The highest security classification of the information with which the Contractor operates under this contract is *[Insert classification here]*.
- G.5. The aspects of the contract which require a Security Classification are:-

Aspect	Security Classification
(provide full and detailed information)	

- G.6. If the contract contains a Condition of Clause referring to “Secret Matter” this Secret matter is defined as the Aspects listed above.
- G.7. The Contractor is responsible for ensuring that the level of protective marking associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this contract, that they are fully understood, and that the required security controls in the contract security conditions can and will be taken to safeguard the material concerned.
- G.8 At the outset of this contract the person identified by the Contractor who will take responsibility for the security of the classified material:
- Name: _____ Role: _____
- G.9 If during the term of the contract the person responsible for the security of the classified material changes, then the Contractor must advise the Client at the earliest opportunity.