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

Order Form

CALL-OFF REFERENCE:	SR879034399
THE BUYER:	HM Revenue & Customs
BUYER ADDRESS	100 Parliament Street London SW1A
THE SUPPLIER:	Equifax Limited
SUPPLIER ADDRESS:	1 Angel Court London EC2R 7HJ
REGISTRATION NUMBER:	7171199

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 17/03/2022. It's issued under the Framework Contract with the reference number RM6226 for the provision of Debt Resolution Services.

CALL-OFF LOT(S):
Lot 2

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

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6226
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6226
        - Joint Schedule 2 (Variation Form and Change Control Procedure)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 7 (Financial Difficulties)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)

- Call-Off Schedules for RM6226
  - Call-Off Schedule 5 (Pricing Details)
  - Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 9 (Security Requirements)
  - Call-Off Schedule 14 (Service Levels)
  - Call-Off Schedule 15 (Call-Off Contract Management)
  - Call-Off Schedule 20 (Call-Off Specification)

5. CCS Core Terms (version 3.0.11)

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:

Special Term 1

HMRC MANDATORY CLAUSES TO ADD TO ALL HMRC CONTRACTS THAT ARE NOT BASED ON HMRC STANDARD CONTRACT TEMPLATES

HM Revenue & Customs

AUTHORITY'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 Framework Schedule 6 Order Form.

C. In case of any ambiguity or conflict, the Authority's mandatory terms in this Framework Schedule 6 Order Form will supersede any other terms in the Agreement.

D. For the avoidance of doubt, the relevant definitions for the purposes of the defined terms set out in the Authority's mandatory terms in this Framework Schedule 6 Order From are the definitions set out below.

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;

"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 Call Off Schedule 5;
"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 UK GDPR;
"Data Protection Legislation"	(a) "the data protection legislation" as defined in section 3(9) of the Data Protection Act 2018; and; (b) all applicable Law about the processing of personal data and privacy;
"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 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 UK 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;

"Tax NonCompliance"	where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC's "Test for Tax NonCompliance", 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;
"UK GDPR"	the UK General Data Protection Regulation, the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
"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 Call Off Schedule 5 of 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.

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.

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 armslength 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 parties agree that the Supplier shall, whether it is the Controller or Processor, in relation to any Personal Data processed in connection with its obligations under the Agreement:

6.1.1 not process or permit to be processed Personal Data outside of the United Kingdom unless the prior explicit written consent of the Authority has been obtained and the following conditions are fulfilled:

(a) the Supplier or any applicable Processor has provided appropriate safeguards in relation to any transfer of the Personal Data (whether in accordance with UK GDPR Article 46 or, where relevant, section 75 of the Data Protection Act 2018) as determined by either the Authority or the Supplier when it is the Controller;

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

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

(d) the Supplier or any applicable Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

6.2 Failure by the Supplier 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).

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 evasion[2];
b. Conduct caught by the General Anti-Abuse Rule[3];
c. Conduct caught by the Halifax Abuse principle[4];
d. Entered into arrangements caught by a DOTAS or VADR scheme[5];
e. Conduct caught by a recognised 'anti-avoidance rule'[5] 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 effected for commercial purposes. 'Targeted

[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.

[5] 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.

AntiAvoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

f. Entered into an avoidance scheme identified by HMRC's published Spotlights list[6];
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:

1. 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) procedure[7]; or,
    2. Has been charged with an offence of fraudulent evasion.
2. 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.
3. 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.
4. In respect of (f) this condition is satisfied without any further steps being taken.
5. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

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.

Annex 2 Form

CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: Calloff Contract entered into between the parties on or around this date ('the Agreement')

DECLARATION:

I solemnly declare that:

[6] 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-schemescurrently-in-the-spotlight

[7] 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.

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:

Special Term 2.

OFFICIAL

CALL-OFF START DATE: 01/04/2022

CALL-OFF EXPIRY DATE: 31/03/2023

CALL-OFF INITIAL PERIOD: 12 months

CALL-OFF OPTIONAL EXTENSION PERIOD N/A

CALL-OFF DELIVERABLES
See details in Call-Off Schedule 20 (Call-Off Specification)

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 £1,166,666 (excl VAT)

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

REIMBURSABLE EXPENSES
None

PAYMENT METHOD
BACS – HMRC use an eTrading Portal Mybuy (provided by SAP Ariba) to manage all ongoing financial transactions with its suppliers

HMRC has a “Purchase Order Mandatory Policy”, Suppliers are required to register on the SAP Ariba Network in order to transact with HMRC via the e-Trading system and to ensure that they will continue to be able to receive purchase orders from and issue invoices to HMRC

BUYER’S INVOICE ADDRESS:
HMRC Invoice Processing Centre
PO Box 2092, J Spur, Barrington Road
Worthing
BN12 9AD

BUYER’S AUTHORISED REPRESENTATIVE
XXXXXXXXXXXXXXX

BUYER’S ENVIRONMENTAL POLICY
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-thegovernment-buying-standards-gbs

BUYER'S SECURITY POLICY
A Baseline Personnel Security Standard (BPSS) pack will be needed for all supplier resources; Security Check (SC) will be required for any Production System access

SUPPLIER'S AUTHORISED REPRESENTATIVE
XXXXXXXXXXXXXXX

SUPPLIER'S CONTRACT MANAGER
XXXXXXXXXXXXXXX

PROGRESS REPORT FREQUENCY
N/A

PROGRESS MEETING FREQUENCY
N/A

KEY STAFF
XXXXXXXXXXXX

KEY SUBCONTRACTOR(S)
Not applicable

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
Not applicable

OFFICIAL

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		Signature:	
Name:	xxxxxxxxx	Name:	xxxxxxx
Role:		Role:	
Date:		Date:	

Joint Schedule 2 (Variation Form and Change Control Procedure)

Part A - Variation Form

This Variation Form shall be used to make a Variation or Change (in accordance with the Change Control Procedure set out in Part B of this Schedule) to the 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	
Implementation Plan / Testing required;		
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation Form 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 Form shall have the meanings given to them in the Contract.

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

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	

Part B Change Control Procedure

This Part B of this Schedule sets out the process to be followed when CCS or the Buyer wishes to make a Change in the way in which the Deliverables or Service is provided by the Supplier.

Definitions

The following definitions apply to this Schedule and are supplemental to those in Joint Schedule 1 (Definitions):

Actual Expenditure	the amount of money spent that a Supplier actually incurred in implementing a Change
Change	a change made to the way in which any Deliverables or Service is provided by the Supplier to the Buyer under the Call Off Contract, which has been requested by the Buyer and agreed with the Supplier as part of the Change Control Procedure;
Change Control Procedure	the processes and procedures to be followed by the CCS or Buyer (as appropriate) and Supplier in proposing, agreeing, executing, delivering, reporting and managing Changes to the Services or Deliverables under the Contract;
Change Implementation Plan	the plan provided by the Supplier to CCS or the Buyer (as appropriate) for the provision of the Deliverables set out in the draft Variation Form sent by the CCS or the Buyer to the Supplier and agreed by the Buyer or CCS (as applicable) in accordance with the Change Control Procedure;
Change Milestone Certificate	the Certificate issued by the Buyer when the Supplier has met all of the requirements of a Change Milestone set out in the Change Implementation Plan which implements the agreed the Change agreed in the Variation Form under the Change Control Procedure;
Change Milestone	an event or task described in the Change Implementation Plan;
Change Satisfaction Certificate	the certificate issued by CCS or the Buyer (as applicable) when the Supplier has met all of the requirements of a Change set out in the Change Implementation Plan in accordance with the Variation Form and the Change Control Procedure;
Change Test Success Criteria	in relation to any Test associated to a Change, the test success criteria for that Test;
Forecast Expenditure	the forecast money to be spent that a Supplier proposes to incur to implement a Change;

1. Variations and Change Management

1.1 Any Variations that do not fall to be a Change shall (including any change to a Debt Type or introduction of a New Debt Type) be undertaken in accordance with Clause 24 (Changing the Contract) of the Core Terms.

1.2 Where a Change is sought, the Parties shall comply with the Change Control Procedure set out in Part B of this Schedule as well as complying with Clause 24 of the Core Terms.

1.3 Where a Change is an Operational Change, the Parties shall comply with Paragraph 6 of this Schedule.

1.4 Any Variation or Change agreed under Paragraphs 1.1 and 1.2 above shall be recorded using the Variation Form in Part A of this Schedule.

Change Control Procedure

2. Approach to Change

2.1 This Schedule sets out a 2-tier Change Control Procedure which shall be used to ensure operational efficiency:

- **Tier 1: Fast Track Change** – to be used where the Buyer requires an immediate solution. The Buyer may request no more than 4 Fast Track Changes in any rolling 12Month period.
- **Tier 2: Standard Change** – to be used where CCS or the Buyer seeks a Change that is not a Fast Track Change.

2.2 All CCS or Buyer requests for a Change must be delivered to the timelines set out in the executed Variation Form, unless otherwise agreed in writing between the relevant Parties. CCS or the Buyer, acting reasonably, will establish the timelines by which any Change shall be delivered by the Supplier. CCS or the Buyer, at their sole discretion may accept an alteration to the timescales in writing.

2.3 **Tier 1: Fast Track Change:** Upon receipt of the Buyer's request for a Change, the Supplier shall provide an Impact Assessment for the proposed Change within 5 Working Days of the date of the Buyer's request. The request shall be in the form of a draft Variation Form. The Buyer shall indicate in the draft Variation Form whether it is seeking to use the Tier 1: Fast Track Change or Tier 2: Standard Change procedure.

2.4 The Buyer and the Supplier may agree in writing to vary Tier 1: Fast Track Change parameters from time to time.

2.5 The Buyer shall be able to make a Tier 1: Fast Track Change request at any time after the satisfactory completion and acceptance of all Change Milestones and Tests regarding the Change Implementation Plan in accordance with Call-Off Schedule 13 (Implementation Plan and Testing). Any Change requests that fall within the Change Implementation Plan period will not amount to a Tier 1: Fast Track Change or Tier 2: Standard Change.

2.6 **Tier 2: Standard Change:** Upon receipt of a Buyer's Change request, the Supplier shall provide an Impact Assessment for the proposed Change within 20 Working Days of the date of issue on the draft Variation Form from CCS or the Buyer (as appropriate), unless otherwise specified in writing by the Buyer in the draft Variation Form.

2.7 If the Supplier has any questions regarding the content of the draft Variation Form submitted by CCS or the Buyer, the Supplier must clarify these with CCS or the Buyer before the Supplier provides the Impact Assessment to CCS or the Buyer within the 5 Working Days for Tier 1: Fast Track Changes, or 20 Working Days for a Tier 2: Standard Change, unless otherwise agreed in writing between the Supplier and CCS or the Buyer (as applicable).

2.8 The Supplier must use their expertise and innovation to provide a solution for delivering the Changes required by CCS or the Buyer within the applicable timeframes and ensuring that CCS or the Buyer's requirements are met.

2.9 Where CCS or the Buyer requires further clarification or amendment to be made to the Impact Assessment to ensure CCS or the Buyer (as applicable) accept the Impact Assessment, the

Supplier must return their response to the further clarification or amendment regarding the Change request within 2 Working Days of receipt for a Tier 1: Fast Track Change or within 5 Working Days of receipt for a Tier 2: Standard Change.

2.10 The Supplier shall monitor and manage all aspects of Change delivery and maintain dialogue with CCS or the Buyer (as appropriate), as to the status of the Change. If the Supplier expects any delays to its delivery the Supplier shall inform CCS or the Buyer (as applicable) of the reason for the delay, why it has or may occur and how long it will take to resolve.

2.11 The Supplier shall work with Subcontractors to ensure that appropriate Change deliverables and timelines are agreed, fully understood and implemented in accordance with the agreed Change as set out in the agreed Variation Form.

2.12 In the case of either a Tier 1: Fast Track Change or a Tier 2: Standard Change, the Supplier shall provide the Buyer with any additional information requested on an Open Book Data basis, including breakdowns of all costs associated with the proposed Change.

2.13 Any Charges Approved by the Buyer associated with delivering the Change shall be calculated using table 4 at Annex 1 of Framework Schedule 3 (Framework Prices**).**

3. Implementing a Change

3.1 Where a Change requires an Implementation Plan, the Variation Form shall include a draft Change Implementation Plan produced by the Supplier detailing at least, as a minimum, one Milestone marking the delivery of the applicable Change.

3.2 The Buyer will issue a Change Milestone Certificate when the Buyer has confirmed that they are satisfied that the relevant Change Milestone has been Achieved.

3.3 The Buyer will only accept the Change as being delivered once it has Approved the final Change Milestone of the Change Implementation Plan.

3.4 The Supplier must monitor its performance against the Change Implementation Plan and the agreed Change Milestones and report its progress to the Buyer.

3.5 The Supplier shall work with all Subcontractors to ensure that appropriate Change Deliverables and timelines are agreed, fully understood and implemented as set out in the agreed Variation Form.

3.6 Where there is a cost Approved for the delivery of a Change, the invoice for that Change can only be submitted for payment by the Supplier, either:

- once CCS or the Buyer has Approved the Change as having been completed satisfactorily and after the final Change Milestone Certificate has been issued; or
- in accordance with the Change Milestones agreed by CCS or the Buyer within the Impact Assessment.

4. Change Testing

4.1 Where CCS or the Buyer requires Testing as part of Change implementation, the Buyer and Supplier shall comply with Call-Off Schedule 13 (Implementation and Testing) Part B (Testing) when developing the Change Implementation Plan. The Buyer shall agree with the Supplier what

and how the Call-Off Schedule 13 Part B (Testing) shall apply relative to the scope and impact of the Change and include this as part of any Change Milestone Criteria.

5. Change Delivery Reporting

5.1 The Supplier shall report upon the progress of all Variations and Changes made Monthly and this must include as a minimum:

- Performance against Service Levels;
- Any risks, issues and mitigations impacting the Change Implementation Plan and Change Milestones; and
- Forecast Expenditure on the Change versus Actual Expenditure on the Change and updated forecast total costs of the Change

Progress shall be reported to:

- CCS as part of the Supplier's MI and reporting obligations set out in Framework Schedule 5 (Management Charges and Information); and
- The Buyer as part of the Supplier's obligations to comply with Call-Off Schedule 1 (Transparency Reporting).

6. Changes permissible outside of the Change Control Procedure

6.1 Where the Buyer requires an Operational Change to an existing operational process or procedure performed by either the Supplier or its Subcontractor, for example,' where Buyer internal policy &/or guidance is updated, resulting in the need to reflect that update in the Supplier guidance, this will not be a Change that requires the Parties to comply with the Change Control Procedure nor to follow the Variation Procedure unless the Operational Change incurs additional cost or materially impact on the Supplier's resources, in which case the Buyer shall comply with the Change Control Procedure.

6.2 Where the Buyer requires an Operational Change to be made, it shall submit a written request disclosing details of the proposed request for Operational Change and the proposed timescales for its completion.

6.3 The Supplier shall prepare a solution for consideration by and Approval of the Buyer, prior to implementation of it by a date agreed.

6.4 The Supplier shall not implement any Operational Change without the Approval of the Buyer.

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.

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 nonrenewal of any of the Insurances.

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

7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority

receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

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

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

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

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following insurance cover from their first Call Off Contract Start Date in accordance with this Schedule:

1.1 **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) – applicable to all 20 Lots; and

1.2 **public liability insurance, professional indemnity insurance, comprehensive crime insurance and cyber insurance** with cover (for a single event or a series of related events and in the aggregate) of, amongst other, amounts not less than those specified in the table below on a per Lot basis:

Lot No.	Service	Public Liability	Professional Indemnity	Comprehensive Crime	Cyber Insurance
1	Collections	£5m	£5m	£5m	£5m
2	a) Data Reports b) Monitoring and Alerts c) Products	£1m	£1m	£1m	n/a
3	Affordability Assessment and Monitoring	£1m	£1m	£1m	n/a
4	FED Advisory	£1m	£1m	£1m	n/a
5	Enforcement	£5m	£5m	£5m	£5m
6	Litigation England and Wales	£2m	£2m	£2m	£2m
7	Litigation Scotland	£2m	£2m	£2m	£2m
8	UK Auctioneers Services London	£1m	£1m	£1m	n/a
9	UK Auctioneers Services South	£1m	£1m	£1m	n/a
10	UK Auctioneers Services Midlands	£1m	£1m	£1m	n/a
11	UK Auctioneers Services North	£1m	£1m	£1m	n/a
12	UK Auctioneers Services Wales	£1m	£1m	£1m	n/a
13	UK Auctioneers Services Northern Ireland	£1m	£1m	£1m	n/a
14	Process Servers	£1m	£1m	£1m	n/a
15	Spend Analytics and Recovery Services (SARS) AP Review	£1m	£1m	£1m	n/a
16	SARS General Compliance Review	£1m	£1m	£1m	n/a
17	SARS Specialist Review Utilities	£1m	£1m	£1m	n/a
18	SARS Specialist Review Utilities	£1m	£1m	£1m	n/a
19	SARS Specialist Review VAT	£1m	£1m	£1m	n/a
20	Managed Enforcement	£5m	£5m	£5m	£5m

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:

Date, Item(s) and Duration of Confidentiality
Date: 14/03/2022 **Details**: commercial detail **Duration of confidentiality**: For the term of the proof of concept

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.

1.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.

1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer (with whom it has entered into a Call Off Agreement and/ or Lease Agreement) and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

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

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

1.3.3 the proposed Key Subcontractor employs unfit persons.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Joint Schedule 7 (Financial Difficulties)

1. Definitions

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

"Credit Rating Threshold"	1 the minimum credit rating level for the Monitored Company as set out in Annex 2 and
"Financial Distress Event"	2 the occurrence or one or more of the following events: a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; d) Monitored Company committing a material breach of covenant to its lenders; e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or f) any of the following: i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract; ii) non-payment by the Monitored Company of any financial indebtedness; iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or

	iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company 3 in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;
"Financial Distress Service Continuity Plan"	4 a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	5 Supplier
"Rating Agencies"	6 the rating agencies listed in Annex 1.

2. When this Schedule applies

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

2.2 The terms of this Schedule shall survive:

2.2.1 under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

2.2.2 under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

3. What happens when your credit rating changes

3.1 The Supplier warrants and represents to CCS that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within five (5) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.

3.3 If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of

the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

$$\frac{A + B + C}{D}$$

where:

A	is the value at the relevant date of all cash in hand and at the bank of the Monitored Company;
B	is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date;
C	is the value at the relevant date of all account receivables of the Monitored]; and
D	is the value at the relevant date of the current liabilities of the Monitored Company.

3.4 The Supplier shall:

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

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

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

4. What happens if there is a financial distress event

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

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

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

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

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

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

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

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

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

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

4.5.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1,

submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

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

4.6 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.64.6.

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

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

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

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

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

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

5.2 If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

6. What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

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

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

ANNEX 1: RATING AGENCIES

Dun & Bradstreet

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	**Credit rating (long term)**
Supplier	XX

Joint Schedule 10 (Rectification Plan)

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

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

Joint Schedule 11 (Processing Data)

Definitions

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

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

Status of the Controller

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

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

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

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

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

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

Where one Party is Controller and the other Party its Processor

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

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

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

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

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

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

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

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

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

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

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures; (c) ensure that :

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

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

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

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

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

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

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

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

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

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

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

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

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

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

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

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

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

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

(f) becomes aware of a Personal Data Breach.

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

9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the

timescales reasonably required by the Controller) including by immediately providing:

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) obtain the written consent of the Controller;

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

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

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

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

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

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

Where the parties are Independent Controllers of Personal Data

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

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

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

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

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

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

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

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

23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying

likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

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

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

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

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

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

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

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

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

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

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

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

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

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

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the 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 18 to 28 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

This Annex shall be completed by each Controller, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: Nicholas De Lacey-Brown

1.2 The contact details of the Supplier's Data Protection Officer are: Adrian Leung, email: UKDPO@Equifax.com

Description	Details
Identity of Controller for each Category of Personal Data	**The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:* ● Business contact details of Supplier Personnel for which the Supplier is the Controller, ● Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller, ● A random sample of data in accordance with Framework Schedule 1, URN 2.0a Table 1, Individual Data Items, supplemented by any additional relevant data sets the Supplier may have access to address a range of individual and tax risks including Under-declaration of income and Nondisclosure
Duration of the Processing	18 months from the effective date
Nature and purposes of the Processing	XXXXXXXX

Type of Personal Data	. XXXXXXXX
Categories of Data Subject	XXXXXXXXXX
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Following completion of the proof of concept the data will be destroyed.

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

Not applicable.

Call-Off Schedule 5 (Pricing Details)

Framework Ref: RM6226 Debt Resolution Services
Project Version: v1.0
Model Version: v3.1

REDACTED

Crown Commercial Service

Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Order Form lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

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

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

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

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

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

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

1.5 The Supplier shall:

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

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

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;

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

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

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

Call-Off Schedule 9 (Security Requirements)

1. **Definitions**

In this Schedule, the following definitions shall apply and be supplemental to those in Joint Schedule 1 (Definitions):

"Accreditation"	the assessment of the Core Information Management System in accordance with Part C of this Schedule by the Buyer or an independent information risk manager/professional appointed by the Buyer, which results in an Accreditation Decision;
"Accreditation Decision"	is the decision of the Buyer, taken in accordance with the process set out in Paragraph 4 of Part C of this Schedule, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"Accreditation Plan"	the Supplier's plan to attain an Accreditation Approval Statement from the Buyer, which is prepared by the Supplier and Approved by the Buyer in accordance with Part C of this Schedule;
“Anti-Malicious Software”	Software that scans for and identifies possible Malicious Software in the ICT Environment;

"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Sites, the Supplier System, and/or any information or data (including the Confidential Information and the Government Data) used by the Buyer, the Supplier or any Subcontractor in connection with this Call-Off Contract; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including copies of such information or data, used by the Buyer, the Supplier and/or any Subcontractor in connection with this Call-Off Contract; and/or (c) any part of the Supplier System ceasing to be compliant with the Certification Requirements,

	in each case as more particularly set out in the Security Requirements in Framework Schedule 1 (Specification) and the Order Form and the Security Requirements;
"Certification Requirements"	the requirements set out in Part E of this Schedule;
“CHECK Service Provider”	a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC Services required by the Paragraph 4.2 of Part C of this Schedule;
“CIMS Subcontractor”	a Subcontractor that provides or operates the whole, or a substantial part, of the Core Information Management System;

"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Buyer has determined in accordance with the Security Requirements;
General Security Requirements	the Security Requirements that shall apply to any Supplier and / or Subcontractor that processes Personal Data;
"Higher Risk Subcontractor"	a Subcontractor that Processes Government Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Call-Off Start Date and the End Date; or (b) Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;
"IT Health Check" (ITHC)	has the meaning given Paragraph 4.2 of Part C of this Schedule;
Incident Management Process	is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the

	Buyer, the Services and/or users of the Services and which shall be prepared by the Supplier in accordance with Paragraph 13.2 of Part A of this Schedule and as set out by the Supplier and Approved by the Buyer within the template set out in Section 23 of Appendix 1 of this Schedule;

"Information Assurance Assessment"	is the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Part B of this Schedule in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Appendix 1 of this Schedule;
"Information Management System"	the Core Information Management System and the Wider Information Management System;
"Information Security Approval Statement"	a notice issued by the Buyer which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the Buyer: (i) is satisfied that the identified risks have been adequately and appropriately addressed; (ii) the Buyer has accepted the residual risks; and (iii) the Supplier may use the Information Management System to Process Government Data;
"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;
"Medium Risk Subcontractor"	a Subcontractor that Processes Government Data, where that data (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Call-Off Start Date and the End Date; and (b) does not include Special Category Personal Data, other than information

	about the access or dietary requirements of the individuals concerned;

"Required Changes Register"	is a register which forms part of the Risk Management Documentation which records each of the changes that the Supplier has agreed with the Buyer to be made to the Core Information System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in the following Paragraphs within: ● 1.3 of Part B; ● 4 of Part C; ● 3 of Part D; together with the date on which each change shall be implemented and the date on which each change was implemented;
"Risk Management Approval Statement"	a notice issued by the Buyer which sets out the information risks associated with using the Core Information Management System and confirms that the Buyer is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer;
"Risk Management Documentation"	is the information and supporting documentation that the Supplier develops and provides to the Buyer when completing section 11 of the Security Management Plan;
"Risk Management Reject Notice"	has the meaning given in Paragraph 4.8.2;
"Security Management Plan"	comprises all information required from the Supplier in order to demonstrate compliance with the Security Requirements that must be presented in the templates set out in Appendix 1;
Security Requirements	the security requirements that the Supplier and each Subcontractor must comply with during the Contract Period as set out in the this Schedule;
"Security Test"	has the meaning given Paragraphs 4 in Part C and Part D of this Schedule;
Security Working Group	the meeting led by the Buyer (or their agent) with the Supplier to discuss the Security Management Plan and any risks, issues and controls the Supplier has put into place to ensure

	they are delivering the Security Requirements. The timing, required attendees and periodicity of the meetings will be defined by the Buyer during implementation, but should be no less than quarterly and should include the Supplier's Staff with the relevant expertise;
"Special Category of Personal Data"	the categories of Personal Data set out in Article 9(1) of GDPR;
"Statement of Information Risk Appetite"	the document that sets-out the type and level of risk that the Buyer is prepared to accept;
"Subcontractor Security Requirements"	any Security Requirements that must be delivered by Subcontractors;
"Vulnerability Correction Plan"	has the meaning given in Paragraph Part C Paragraph 4.3.3.1 of this Schedule;
"Wider Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data which have not been determined by the Buyer to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

2. Part A Introduction

2.1. This Schedule sets out:

2.1.1. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of Government Data, the Services and the Information Management System;

2.1.2. the Certification Requirements applicable to the Supplier and each of those Subcontractors which Processes Government Data;

2.1.3. the Security Requirements with which the Supplier must comply, which are dependent upon the applicable Lot(s) awarded to the Supplier under the Framework Contract;

2.1.4. the tests which the Supplier shall conduct on the Information Management System during the Term;

2.1.5. the Supplier's obligations to:

2.1.5.1. return or destroy Government Data on the expiry or earlier termination of this CallOff Contract; and

2.1.5.2. prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 8; and

2.1.5.3. report Breaches of Security to the Buyer.

2.1.6. the applicable Tier of Security Requirements required to be complied with by the Supplier are summarised in Table 1 below:

Table 1:

Tier	Lot	Summary Security Requirements	Certification Requirements
1.	1	<u>General Security Requirements (Part B) plus PSC Accreditation (Part C)</u> The Supplier is also required to: a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request .	ISO 27001:2017 and Cyber Essentials (CE) + and PCI-DSS
2.	5, 6, 7, 20	<u>General Security Requirements (Part A) plus PSC Assurance (Part D) for Lot 20</u> The Supplier is also required to: a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request.	ISO 27001:2017 and CE+ and PCIDSS

3.	2, 3, 8, 9, 10, 11, 12, 13, 14	General Security Requirements (Part B)	ISO 27001:2017 and CE+
4.	4, 15, 16, 17, 18, 19	General Security Requirements (Part B) when handling Personal Data, otherwise N/A	CE

3. **Principles of Security**

3.1. The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently on the security of:

3.1.1. the Sites;

3.1.2. the Supplier System;

3.1.3. the Information Management System, Core information Management System and Wider Information Management System, as applicable; and

3.1.4. the Services.

3.2. Notwithstanding the involvement of the Buyer in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Government Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:

3.2.1. the security, confidentiality, integrity and availability of the Government Data whilst that Government Data is under the control of the Supplier or any of its Subcontractors; and

3.2.2. the security of the Information Management System.

3.3. The Supplier shall:

3.3.1. comply with the Security Requirements in this Schedule; and

3.3.2. ensure that each Subcontractor that Processes Government Data complies with the Subcontractor Security Requirements in this Schedule.

3.4. The Supplier shall provide the Buyer with access to Supplier Staff responsible for information assurance to facilitate the Buyer's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

3.5. The Buyer may at its sole discretion appoint an agent to act on it’s behalf with regards to its engagement with the Supplier regarding the Security Requirements.

Part B General Security Requirements

1. **The Security Management Plan**

1.1 The Security Management Plan includes details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement.

1.2 The Supplier shall complete the Security Management Plan Template (Appendix 1) detailing how they will deliver the Security Requirements and the necessary information required for the applicable Tier(s) for the Lot(s) awarded to the Supplier. Any element that does not apply or only partially applies should be explained within the Template. If a Supplier is delivering Services in respect of more than 1 Lot, it must complete a separate Security Risk Management Template for each Lot.

1.3 Where there has been a Variation or Change to the Services which affects any aspect of the Security Requirements, CCS and the relevant Buyers must be notified immediately in writing of this fact and the extent of its effect or believed effect on the Security Requirements and / or the Tier of the Security Requirements that the Supplier should apply to the Service (actual or potential).

1.4 The Supplier shall complete the Security Management Plan to demonstrate and document how they comply with the Security Requirements. A draft Security Management Plan shall be made available to the Buyer prior to the Call-Off Contract Effective Date unless already Approved by the Buyer.

1.5 The Security Management Plan should be provided to the Buyer in accordance with the Buyer's requirements and as set out within the Implementation Plan, but in any case, unless already Approved by the Buyer, this should be prior to the Service Effective Date.

2. **Security Classification of Information**

2.1 If the provision of the Services requires the Supplier to Process Government Data which is classified as: OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

3. **End User Devices**

3.1 The Supplier shall ensure that any Government Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement.

3.2 The Supplier shall ensure that any device which is used to Process Government Data meets all of the Security Requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security

3.3 The Supplier must ensure that their EUD's require all Supplier Staff to authenticate themselves before gaining access to the device. All the Supplier's EUD's must encrypt all data at rest using a reputable full disk encryption solution that has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement. The Supplier's EUD's must be configured to automatically lock the screen after a period of inactivity and this must be agreed with the Buyer in writing.

4. Location of Government Data

4.1 The Supplier shall not and shall procure that none of its Subcontractors Process Government Data outside the UK without the Approval of the Buyer, which may be subject to conditions and that it shall comply with Joint Schedule 11 (Processing Data).

5. Vulnerabilities and Corrective Action

5.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Government Data.

5.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability.

5.3 The Supplier shall utilise scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

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

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

5.4 Subject to Paragraph 5.5, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

5.4.1 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

5.4.2 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

5.4.3 60 days after the public release of patches for those vulnerabilities categorised as 'Other'.

5.5 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 5.4 shall be extended where:

5.5.1 the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 5.4 if the vulnerability becomes exploitable within the context of the Services;

5.5.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer;

5.5.3 the Buyer Approves to a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan; or

5.5.4 the Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Contract Period, unless otherwise Approved by the Buyer. All COTS Software should be no more than N-1 versions behind the latest software release.

6. **Networking**

6.1 The Supplier shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted using TLS version 1.2 as a minimum.

7. **Personnel Security**

7.1 All Supplier Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

7.2 The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Government Data or data which is classified as OFFICIAL-SENSITIVE.

7.3 The Supplier shall not permit Supplier Staff who fail the security checks required by Paragraphs 7.1 and 7.2 to be involved in the management and/or provision of the Services except where the Buyer Approves the involvement of the named individual in the management and/or provision of the Services.

7.4 The Supplier shall ensure that Supplier Staff are only granted such access to Government Data as is necessary to enable the Supplier Staff to perform their role and to fulfil their responsibilities.

7.5 The Supplier shall ensure that Supplier Staff who no longer require access to the Government Data (e.g. they cease to be employed by the Supplier or any of its Subcontractors), have their rights to access the Government Data revoked within 1 Working Day

8. **Identity, Authentication and Access Control**

8.1 The Supplier shall operate an access control regime to ensure:

8.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

8.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

8.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require to perform the Services under the Contract.

8.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such records available to the Buyer on request.

9. **Audit and Protective Monitoring**

9.1 The Supplier shall collect audit records which relate to security events in the Core Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Core Information Management System, to enable the identification of (without limitation) changing access trends, any unusual

patterns of usage and/or accounts accessing higher than average amounts of Government Data.

9.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

9.3 The retention periods for audit records and event logs must be agreed with the Buyer and documented in the Security Management Plan.

10. **Secure Architecture**

10.1 The Supplier shall design the Core Information Management System in accordance with:

10.1.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digitalservices-main;

10.1.2 the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main ; and

10.1.3 the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

11. **Malicious Software**

11.1 The Supplier shall install and maintain Anti-Malicious Software or procure that AntiMalicious Software is installed and maintained on any part of the Information Management System which may Process Government Data and ensure that such AntiMalicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

11.2 If Malicious Software is found, the Parties shall cooperate 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 Services to their desired operating efficiency.

11.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 11.1 shall be borne by the Parties as follows:

11.3.1 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 the Data was provided to

the Supplier, unless the Buyer had instructed the Supplier to quarantine and check the data for Malicious Software and the Supplier had failed to do so, and

11.3.2 by the Buyer, in any other circumstance. 12. **Data Destruction or Deletion**

12.1 The Supplier shall:

12.1.1 prior to securely sanitising any Government Data or when requested the Supplier shall provide the Buyer with two copies of all Buyer Data in an agreed open format;

12.1.2 have documented processes to ensure the availability of Government Data in the event of the Supplier ceasing to trade;

12.1.3 securely erase in a manner agreed with the Buyer any or all Government Data held by the Supplier when requested to do so by the Buyer;

12.1.4 securely destroy in a manner agreed with the Buyer all media that has held Government Data at the end of life of that media in accordance with any specific requirements in this Call-Off Contract and, in the absence of any such requirements, as agreed by the Buyer in writing; and

12.1.5 implement processes which address the CPNI and NCSC guidance on secure sanitisation.

13. **Breach of Security**

13.1 If either Party becomes aware or reasonably suspects of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

13.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

13.2.1 immediately take all reasonable steps necessary to:

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

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause failure;

13.2.2 as soon as reasonably practicable and, in any event, within twelve (12) hours following the Breach of Security or attempted Breach of Security, the Supplier must

provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis as required by the Buyer.

13.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Subcontractors and/or all or any part of the Information Management System, with this Call-Off Contract, then such remedial action shall be undertaken and completed at no additional cost to the Buyer.

14. **Security Monitoring and Reporting**

14.1 The Supplier shall:

14.1.1 monitor the delivery of assurance activities;

14.1.2 maintain and update the Security Management Plan in accordance with Paragraph

1;

14.1.3 agree a document which presents the residual security risks to inform the Buyer's decision on whether or not to give Approval to the Supplier to Process, store and transit the Government Data;

14.1.4 monitor security risk impacting upon the operation of the Service;

14.1.5 report Breaches of Security in accordance with the approved Incident Management Process; and

14.1.6 agree with the Buyer the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Buyer within 30 days of the Start Date of this Call-Off Contract.

Part C Accreditation requirements

1. **This Part sets out:**

1.1 The Accreditation arrangements that the Supplier must implement and comply with when providing the Services and performing its other obligations under this Call-Off Contract. These are required to ensure the security of the Government Data, the ICT Environment, the Services and the Information Management System, which are in addition to the requirements set-out in Parts A, B and E and Appendix 1 and 2 of this Schedule.

1.2 To facilitate the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Information Management System and otherwise.

1.3 The Supplier shall provide access to the Supplier Staff responsible for information assurance and the Buyer shall provide access to its Personnel responsible for information assurance, at reasonable times upon reasonable written notice.

2. **Information Management System**

2.1 The Information Management System comprises the Core Information Management System and the Wider Information Management System.

2.2 The Buyer shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Buyer to make such determination, the Supplier shall provide the Buyer with such documentation and information that the Buyer may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Subcontractor to Process Government Data together with the associated information management system (including organisational

structure, controls, policies, practices, procedures, processes and resources). The Buyer shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

2.3 The Supplier shall reproduce the Buyer's decision as a diagram documenting the Core Information Management System, the Wider Information Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.

2.4 Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the

Wider Information Management System shall be notified and processed in accordance with Clause 24 of the Core Terms (Changing the contract).

3. **Statement of Information Risk Appetite and Security Requirements**

3.1 The Supplier acknowledges that the Buyer has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services ("**Statement of Information Risk Appetite**").

3.2 The Buyer's Security Requirements in respect of the Core Information Management System shall be set out in Appendix 1 (below).

4. **Accreditation of the Core Information Management System**

4.1 The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 4.

4.2 The Supplier acknowledges that the purpose of Accreditation is to ensure that:

4.2.1. the Security Management Plan accurately represents the Core Information Management System;

4.2.2. the Accreditation Plan, if followed, provides the Buyer with sufficient confidence that the CIMS will meet the requirements of the Security Requirements and the Statement of Risk Appetite; and

4.2.3. the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Risk Appetite and Security Requirements.

4.3 The Accreditation shall be performed by the Buyer or by representatives appointed by the Buyer.

4.4 In addition to any obligations imposed by Call-Off Schedule 13 (Implementation Plan and Testing), the Supplier must ensure that its

Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Subcontractors, from the Call-Off Contract Start Date.

4.5 By the date specified in the Implementation Plan, the Supplier shall prepare and submit to the Buyer the risk management documentation for the Core Information Management System, which shall be subject to approval by the Buyer in accordance with, Part B Paragraph 5 (the "**Security Management Plan**").

4.6 The Supplier must provide, by the date by which the Supplier is required to have received a Risk Management Approval Statement from the Buyer together with:

4.6.1. details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in

order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 4.8.1.

4.6.2. a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;

4.6.3. a completed ISO 27001:2013 Statement of Applicability for the Core Information

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

4.6.4. unless such requirement is waived by the Buyer, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Call-Off Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services including:

4.6.4.1. the Required Changes Register;

4.6.4.2. evidence that the Supplier and each applicable Subcontractor is compliant with the Certification Requirements;

4.6.4.3. a Personal Data Processing Statement; and

4.6.4.4. the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between the two created under Paragraph 3.2.

4.7 To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Buyer and its authorised representatives with:

4.7.1. access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and

4.7.2. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require, to enable the Buyer to establish that the

Core Information Management System is compliant with the Security Management Plan.

4.8 The Buyer shall, by the relevant date set out in the Accreditation Plan, review the Security Management Plan and issue to the Supplier either:

4.8.1. a Risk Management Approval Statement which will then form part of the Security Management Plan, confirming that the Buyer is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer; or

4.8.2. a rejection notice stating that the Buyer considers that the identified risks to the Core Information Management System have not been adequately or appropriately addressed or the residual risks to the Core Information Management System have not been reduced to the level anticipated by the Statement of Information Risk Appetite, and the reasons why (**"Risk Management Rejection Notice"**).

4.9 If the Buyer issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:

4.9.1. address all of the issues raised by the Buyer in such notice;

4.9.2. update the Security Management Plan, as appropriate, and

4.9.3. notify the Buyer that the Core Information Management System is ready for an Accreditation Decision.

4.10 If the Buyer issues a two or more Risk Management Rejection Notices, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

4.11 Subject to Paragraph 4.10, the process set out in Paragraphs 4.9 shall be repeated until such time as the Buyer issues a Risk Management Approval Statement to the Supplier or terminates this Call-Off Contract.

4.12 The Supplier shall not use the Core Information Management System to Process Government Data prior to receiving a Risk Management Approval Statement.

4.13 The Supplier shall keep the Core Information Management System and Security Management Plan under review and shall update the Security Management Plan annually in accordance with this Paragraph 4 and the Buyer shall review the

Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 4.9.

4.14 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

4.14.1. a significant change to the components or architecture of the Core Information Management System;

4.14.2. a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;

4.14.3. a change in the threat profile;

4.14.4. a Subcontractor failure to comply with the Core Information Management System code of connection;

4.14.5. a significant change to any risk component; and/or

4.14.6. a significant change in the quantity of Personal Data held within the Core Information Management System.

4.15 Where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to Process Special Category Personal Data, other than data relating to accessibility or dietary requirements relating to an individual:

4.15.1. a proposal to change any of the Sites from which any part of the Services are provided; and

4.15.2. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns; and

4.15.3. update the Required Changes Register and provide the updated Required Changes Register to the Buyer for review and Approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Buyer.

4.16 If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Buyer, such failure shall constitute a material Default and the Supplier shall:

4.16.1. immediately cease using the Core Information Management System to Process Government Data until the Default is remedied, unless directed otherwise .by the Buyer in writing and then it may only continue to Process Government Data in accordance with the Buyer's written directions; and

4.16.2. where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Buyer and, should the Supplier fail to remedy the Default within such timescales, the Buyer may terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms

4.17 The Supplier shall review each Change request against the Security Management Plan to establish whether the documentation would need to be amended should such Change request be agreed and, where a Change request would require an amendment to the

Security Management Plan, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change request for consideration and Approval by the Buyer.

4.18 The Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan and carrying out any remedial action required by the Buyer as part of the Accreditation process.

5. **Security Testing**

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

5.1.1. procure testing of the Core Information Management System by a CHECK Service Provider (an "**IT Health Check**"):

5.1.1.1. prior to it submitting the Security Management Plan to the Buyer for an Accreditation Decision;

5.1.1.2. if directed to do so by the Buyer; and

5.1.1.3. once every 12 Months during the Call-Off Contract Period:

5.1.1.4. conduct vulnerability scanning and assessments of the Core Information Management System Monthly;

5.1.1.5. conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Subcontractors of a critical vulnerability alert from a supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and

5.1.1.5.1. conduct such other tests as are required by:

5.1.1.5.2. any Vulnerability Correction Plans;

5.1.1.5.3. the ISO27001 certification requirements;

5.1.1.5.4. the Security Management Plan; and

5.1.1.5.5. The Buyer following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

(each a "**Security Test**").

5.2 The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Security Test.

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

5.3.1. agree with the Buyer the aim and scope of the IT Health Check;

5.3.2. promptly, and in any case no later than 10 Working Days, following receipt of each IT Health Check report, provide the Buyer with a copy of the IT Health Check report

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

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

5.3.4.1. how the vulnerability will be remedied;

5.3.4.2. the date by which the vulnerability will be remedied;

5.3.4.3. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer,

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

5.3.4.4. comply with the Vulnerability Correction Plan; and

5.3.4.5. conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

5.4 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.

5.5 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 5.3, the Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case no later than 10 Working Days, after completion of each Security Test.

5.6 The Buyer and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information Management System and/or the Supplier's compliance with the Security Management Plan ("**Buyer Security Tests**"). The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Buyer Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature and purpose of the Buyer Security Test.

5.7 The Buyer shall notify the Supplier of the results of such Buyer Security Tests after completion of each Buyer Security Test.

5.8 The Buyer Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If a Buyer Security Test causes Supplier NonPerformance, the Buyer Security Test shall be treated as an Authority Cause for the purposes of Clause 5.1 of the Core Terms, except where the root cause of the Supplier Non-Performance was a weakness or vulnerability exposed by the Buyer Security Test.

5.9 Without prejudice to the provisions of Paragraph 5.3, where any Security Test carried out pursuant to this Paragraph 5 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the Core Information Management System and/or the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's Approval, the Supplier shall implement such changes to the Core Information Management System and/or the Security Management

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

5.10 If the Buyer unreasonably withholds its Approval to the implementation of any changes proposed by the Supplier to the Security Management Plan in accordance with Paragraph 5.9 above, the Supplier shall not be deemed to be in breach of this Call-Off Contract to the extent it can be shown that such breach:

5.10.1. has arisen as a direct result of the Buyer unreasonably withholding its Approval to the implementation of such proposed changes; and

5.10.2. would have been avoided had the Buyer given its Approval to the implementation of such proposed changes.

5.11 For the avoidance of doubt, where a change to the Core Information Management System and/or the Security Management Plan is required to remedy non-compliance with the Risk Management Documentation, the Security Requirements and/or any obligation in this Call-Off Contract, the Supplier shall effect such change at its own cost and expense.

5.12 If any repeat Security Test carried out pursuant to Paragraph 5.3 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

5.13 The Supplier shall, by 31 March of each Financial Year during the Call-Off Contract Period, provide to the Buyer a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

5.13.1. the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Call-Off Contract; and

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

6. Vulnerabilities and Corrective Action

6.1 In addition to the requirements within Part B, the Supplier shall:

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

6.1.2. promptly notify NCSC of any actual or sustained attempted Breach of Security;

6.1.3. ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

6.1.4. ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Call-Off Contract Period;

6.1.5. pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;

6.1.6. from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent Month during the Call-Off Contract Period, provide the Buyer with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Part B Paragraph

5.4 for applying patches to vulnerabilities in the Core Information Management System;

6.1.7. propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;

6.1.8. remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Core Information Management System); and

6.1.9. inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.

6.2 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Part B Paragraph 5.4, the Supplier shall immediately notify the Buyer.

6.3 If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Part B Paragraph 5.3, such failure shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

PART D Assurance requirements

1. This Part D sets out the Assurance arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of the Government Data and the Information Management System.

1.1 The Supplier must comply with the Assurance arrangements in addition to the other Security Requirements as set out within Parts A and B and E of this Schedule and Appendix 1 (Security Management Plan).

2. **Information Security Approval Statement**

2.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Sub-contractors from the CallOff Start Date.

2.2 The Supplier may not use the Information Management System to Process Government Data unless and until:

2.2.1 the Supplier has procured the conduct of an ITHC of the Supplier System by a CHECK Service Provider in accordance with Paragraph 4; and

2.2.2 the Buyer has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 2.

2.3 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule and the CallOff Contract in order to ensure the security of the Government Data and the Information Management System.

2.4 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which comprises:

2.4.1 an Information Assurance Assessment;

2.4.2 the Required Changes Register;

2.4.3 the Personal Data Processing Statement; and

2.4.4 the Incident Management Process.

2.5 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:

2.5.1 an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Government Data; or

2.5.2 a rejection notice which shall set out the Buyer's reasons for rejecting the Security Management Plan.

2.6 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Buyer's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Buyer for review within 10 Working Days or such other timescale as agreed with the Buyer.

2.7 The Buyer may require and the Supplier shall provide the Buyer and its authorised representatives with:

2.7.1 access to the Supplier Staff;

2.7.2 access to the Information Management System to Audit the Supplier and its Subcontractors' compliance with this Call-Off Contract;

2.7.3 such other information and/or documentation that the Buyer or its authorised representatives may reasonably require;

2.7.4 assistance to the Buyer to establish whether the arrangements which the Supplier and its Subcontractors have implemented in order to ensure the security of the Government Data and the Information Management System are consistent with the representations in the Security Management Plan; and

2.7.5 the Supplier shall provide the access required by the Buyer in accordance with this Paragraph within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

3. **Compliance Reviews**

3.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

3.2 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

3.2.1 a significant change to the components or architecture of the Information Management System;

3.2.2 a new risk to the components or architecture of the Service;

3.2.3 a vulnerability to the components or architecture of the Service which is classified '**Medium**', '**High**', '**Critical**' or '**Important**' in accordance with the classification methodology set out in Paragraph 5 of Part B to this Schedule;

3.2.4 a change in the threat profile;

3.2.5 a significant change to any risk component;

3.2.6 a significant change in the quantity of Personal Data held within the Service;

3.2.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

3.2.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

3.3 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Buyer for review and Approval.

3.4 Where the Supplier is required to implement a change, including any change to the Information Management System the Supplier shall effect such change at its own cost and expense.

4. **Security Testing**

4.1 The Supplier shall, at its own cost and expense procure and conduct:

4.1.1 testing of the Information Management System by a CHECK Service Provider ("**ITHC**"); and

4.1.2 such other security tests as may be required by the Buyer; and

4.1.3 the Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Buyer for review in accordance with Paragraph 3; and it shall repeat the ITHC not less than once every 12 Months during the Term and submit the results of each such test to the Buyer for review in accordance with this Paragraph.

4.2 In relation to each ITHC, the Supplier shall:

4.2.1 agree with the Buyer the aim and scope of the ITHC;

4.2.2 promptly, and no later than 10 Working Days, following the receipt of each ITHC report, provide the Buyer with a copy of the full report;

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

(a) prepare a remedial plan for Approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the ITHC report:

(i) how the vulnerability will be remedied;

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

(iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

4.3 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Buyer.

4.4 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique] that has the potential to affect the security of the Information Management System, the Supplier shall within days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Buyer with a copy of the test report and:

4.4.1 propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and

4.4.2 where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

4.5 The Supplier shall conduct such further tests of the Supplier System as may be required by the Buyer from time to time to demonstrate compliance with its obligations set out this Schedule and the Call-Off Contract.

4.6 The Supplier shall notify the Buyer immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 5 of Part B to this Schedule.

Part E Certification requirements

Certification Requirements

1. Supplier Requirements

1.1. The Supplier shall as applicable to the Lot and the associated Security Tier, ensure, at all times during the Call-Off Contract Period, that it is certified as compliant with:

1.1.1. ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

1.1.2. Cyber Essentials or Cyber Essentials PLUS as applicable to the Lot and

Security Tier of the Service, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme), and shall provide the Buyer with a copy of each such certificate of compliance before the Supplier or the relevant Subcontractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Government Data.

2. **Payment Card Industry Data Security Standard (PCI DSS) Compliance**

2.1. All Suppliers and / or Subcontractors that are a payment processor must be, and remain, appropriately certified according to the Payment Card Industry Data Security Standard requirements throughout the term of the Contract

2.2. Where the Supplier and / or Subcontractor intends to accept payments, restricted to at sale only, by debit/credit card the Supplier and / or Subcontractor must have either:

2.2.1. been certified by a Qualified Security Assessor as being compliant with the PCI DSS version 1.1;

2.2.2. completed an internal self-assessment and will adhere at all times to the terms of the PCI DSS and will notify the Client promptly in writing of any changes in the Contractor's certification.

2.3. The Supplier / Subcontractor must validate compliance in the manner deemed appropriate by the card scheme industry on an annual basis and provide the Buyer with written evidence of compliance annually.

2.4. The Supplier / Subcontractor will be responsible for any costs incurred to attain and maintain compliance with PCI DSS.

2.5. The Supplier / Subcontractor must meet all PCI DSS requirements, on a continuing basis, including but not limited to any subsequent versions of the PCI DSS.

2.6. The Supplier / Subcontractor must be responsible for the security of all cardholder Data in their possession and must protect data by the card scheme industry standard on an annual basis and provide the Buyer access hosted environment and data when necessary.

2.7. The Supplier / Subcontractor must notify the Buyer and the card scheme industry immediately if it knows or suspects that there has been, or will be, a breach of the security of Cardholder Data or of the PCI DSS.

2.8. The Supplier / Subcontractor must indemnify the Buyer, its subsidiaries, affiliates, officers, employees and agents from and against all actions, demands, costs, Losses, whatsoever incurred by it or them arising out of or in connection with the Supplier's noncompliance with, or breach of, the PCI DSS or breach of Cardholder Data security.

2.9. The Supplier / Subcontractor must cease taking payments, by Debit Card / Credit Card, on behalf of the Buyer in the event that the Supplier becomes non-compliant with, or suffers a breach of, the PCI DSS or breach of Cardholder Data security.

3. **Subcontractor Requirement**

3.1. Notwithstanding anything else in this Contract, a CMIS Subcontractor shall be treated for all purposes as a Key Subcontractor.

3.2. In addition to the obligations contained in Joint Schedule 6 (Key Subcontractors), the Supplier must ensure that the Key Subcontract with each CIMS Subcontractor.

3.3. contains obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Call-Off Schedule 9 (Security Requirements);

3.3.1. provides for the Buyer to perform Accreditation of any part of the Core Information Management System that the CIMS Subcontractor provides or operates which is not otherwise subject to Accreditation under this Call-Off Schedule 6 (Security Requirements).

3.4. The Supplier shall ensure that each Higher Risk Subcontractor is certified as compliant, and the Supplier shall provide the Buyer with a copy of each such certificate of compliance before the Higher-Risk Subcontractor shall be permitted to receive, store or Process Government Data, with either:

3.4.1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or

3.4.2. Cyber Essentials PLUS, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme),

3.5. The Supplier shall ensure that each Medium Risk Subcontractor is certified compliant with Cyber Essentials, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme).

3.6. The Supplier shall notify the Buyer as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Subcontractor ceases to be compliant with the Certification Requirements and, on request from the Buyer, shall or shall procure that the relevant Subcontractor shall:

3.6.1. immediately ceases using the Government Data; and

3.6.2. procure that the relevant Subcontractor promptly returns, destroys and/or erases the Government Data in accordance with Security Requirements.

3.7. The Buyer may agree to exempt, in whole or part, the Supplier or any Subcontractor from the Certification Requirements. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

Appendix 1

Security Management Plan Template

DRS Call-Off Schedule 9 (Appendix 1)

Security Management Plan Template

REDACTED

Framework Ref: RM6226 Debt Resolution Services

Project Version v2.1
Model Version [1.0].

66413318 v3

Call-Off Schedule 14 (Service Levels)

1. Definitions

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

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Credits"	1 any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	2 has the meaning given to it in the Order Form; 3
"Service Level Failure"	4 means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	5 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	6 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

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

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

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

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

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

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

2.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

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

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

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

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

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

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

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

2.5.3 there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

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

3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("Compensation for Critical Service Level Failure"),

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

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur, the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

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

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

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

2. Service Credits

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

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

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

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Accurate and timely billing of Buyer	Accuracy /Timelines	at least 100% at all times	N/A	N/A
Delivery of the data sets and invoicing for the costs prior to 31/03/2022	Accuracy/ Timelines	at least 100% at all times	N/A	N/A

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

[Example:

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

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

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

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

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

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

3.2.3 details of any Critical Service Level Failures;

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

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

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

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

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

3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

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

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

3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

4. Satisfaction Surveys

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

Call-Off Schedule 15 (Call-Off Contract Management)

1. DEFINITIONS

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

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. PROJECT MANAGEMENT

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

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

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

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

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

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

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

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

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

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

4. ROLE OF THE OPERATIONAL BOARD

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

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

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

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

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

5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

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

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues;

and

5.2.3 monitoring and controlling project plans.

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

5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

Annex: Contract Boards

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

None required

Call-Off Schedule 20 (Call-Off Specification)

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

SCHEDULE A SPECIFICATION

PROOF of CONCEPT FOR CRA BULK DATA