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

CALL-OFF REFERENCE:	**project_4038 / con_14134**
THE BUYER:	**The Secretary of State for Education**
BUYER ADDRESS	**20 Great Smith St, Westminster, London SW1P 3BT**
SUPPLIER REFERENCE	**RM3808-1303**
THE SUPPLIER:	**Vodafone Limited**
SUPPLIER ADDRESS:	**Vodafone House, The Connection, Newbury, RG14 2FN**
REGISTRATION NUMBER:	**01471587**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 1st June 2022.
It is issued under the Framework Contract with the reference number RM3808 for the provision of Network Services.

CALL-OFF LOT(S):

Lot 6: Mobile Voice and Data Services

CALL-OFF INCORPORATED TERMS

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

1. This Order Form including the Call-Off Special Terms and Call-Off special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3808
3. The following Schedules in equal order of precedence:
    - Joint Schedules for framework reference number RM3808
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)

- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

- Call-Off Schedules for Project_4038
  - Call-Off Schedule 1 (Transparency Reports)
  - Call-Off Schedule 2 (Staff Transfer) – Schedule wording not present in the body of the contract for ease of review purposes, however it remains part of this Order Form and applicable.
  - Call-Off Schedule 3 (Continuous Improvement)
  - Call-Off Schedule 5 (Pricing Details)
  - Call-Off Schedule 6 (ICT Services)
  - Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - Call-Off Schedule 9 (Security)
  - Call-Off Schedule 10 (Exit Management)
  - Call-Off Schedule 11 (Installation Works)
  - Call-Off Schedule 13 (Implementation Plan and Testing)
  - Call-Off Schedule 14 (Service Levels)
  - Call-Off Schedule 15 (Call-Off Contract Management)
  - Call-Off Schedule 16 (Benchmarking)
  - Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3. 0.4)
5. Joint Schedule 5 (Corporate Social Responsibility)

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:
To be advised if required.

CALL-OFF START DATE	1st June 2022
CALL-OFF EXPIRY DATE	31st May 2024
CALL-OFF INITIAL PERIOD	2 Years
CALL-OFF OPTIONAL EXTENSION PERIOD	1 Year

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION
30 days without cause.

CALL-OFF DELIVERABLES
See details in Call-Off Schedule 20 (Call-Off Specification) and Statement of Requirements.

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 [redacted] of Estimated Charges in the first 12 months of the Contract.

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

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4 and 5 in Framework Schedule 3 (Framework Prices).

The Charges will not be impacted by any change to the Framework Prices.

REIMBURSABLE EXPENSES
Not recoverable

PAYMENT METHOD
The Supplier shall submit electronic invoices to the Buyer monthly in arrears, directly to the billing address(es) as per the Buyer's order. The Supplier shall invoice the Buyer for Goods and for Services in accordance with Call-Off Schedule 5 (Pricing Details). Payment to be made by BACS payment.

BUYER'S INVOICE ADDRESS:
[redacted] and [redacted]

BUYER'S AUTHORISED REPRESENTATIVE
[redacted] [redacted]
Head of End User Compute and Onsite Support
[redacted]Piccadilly Gate, Store Street, Manchester M1 2WD

BUYER'S ENVIRONMENTAL POLICY
Not Applicable

ADDITIONAL INSURANCES
Details of Additional Insurances required in accordance with Joint Schedule 3 (Insurance Requirements).

GUARANTEE

The Financial Viability and Risk Assessment completed by the Buyer on the Supplier has provided the necessary financial information to confirm the Supplier's financial stability without the need to provide an additional Guarantee.

SOCIAL VALUE COMMITMENT
See details is Joint Schedule 5 (Corporate Social Responsibility).

STAFF TRANSFER
The following parts of Call-Off Schedule 2 (Staff Transfer) shall apply:
Part C (No Staff Transfer On Start Date).
Part E (Staff Transfer on Exit) will apply to every Contract.

QUALITY PLAN
Not applicable.

MAINTENANCE OF ICT ENVIRONMENT
Not applicable.

BUSINESS CONTINUITY AND DISASTER RECOVERY
In accordance with Call-Off Schedule 8 (Business Continuity and Disaster Recovery) Part B, the Supplier shall prepare and deliver a bespoke BCDR Plan for the Buyer's written approval within 3 months of the contract Start Date.

SECURITY REQUIREMENTS
In accordance with Call-Off Schedule 9, Part B (Long Form Security Requirements) applies.

BUYER'S SECURITY POLICY
See details in Call-Off Schedule 9 (Security) Annex 1.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)
Not applicable.

CLUSTERING
Not applicable.

SERVICE LEVELS AND SERVICE CREDITS
Service Credits will accrue in accordance with Call-Off Schedule 14 Part B (Long Form Service Levels and Service Credits).

The required Service Maintenance Level is Level 1.

The Service Credit Cap is in accordance with Call-Off Schedule 14 (Service Levels).

PERFORMANCE MONITORING

See details in Call-Off Schedule 14 (Service Levels) Part C and Annex 1 to Part C.

Additional performance monitoring required is not required.

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

SUPPLIER'S CONTRACT MANAGER
[redacted]
Frameworks Manager
[redacted]

PROGRESS REPORT FREQUENCY
As described in Call-Off Schedule 1 (Transparency Reports).

PROGRESS MEETING FREQUENCY
Monthly.

OPERATIONAL BOARD
In accordance with Call-Off Schedule 15 (Call-Off Contract Management) the Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established.

KEY STAFF
See details in Call-Off Schedule 7 (Key Supplier Staff).

KEY SUBCONTRACTOR(S)
None.

COMMERCIALLY SENSITIVE INFORMATION
As described in Joint Schedule 4 (Commercially Sensitive Information).

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

Joint Schedule 2 (Variation Form)

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

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

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by the Buyer**.**

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

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

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

Signature	
Date	
Name (in Capitals)	
Title	

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

Signature	
Date	
Name (in Capitals)	
Title	

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 non-renewal of any of the Insurances.

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

7. Insurance claims

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

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

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

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

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

ANNEX: Required Insurances

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

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

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

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

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

Joint Schedule 4 (Commercially Sensitive Information)

2. What is the Commercially Sensitive Information?

2.1 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.

2.2 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).

2.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	[redacted]	[redacted]	[redacted]

Joint Schedule 5 (Corporate Social Responsibility)

3. What we expect from our Suppliers

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

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

3.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such reasonable corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time. Any necessary changes to the relevant Call-Off Contract shall be enacted via the Variation Procedure.

4. Equality and Accessibility

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

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

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

5. Modern Slavery, Child Labour and Inhumane Treatment

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

5.1 The Supplier:

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

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

5.1.3 warrants and represents that it has not been convicted of any slavery or human tracking offenses anywhere around the world.

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

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

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

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

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

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

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

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

5.1.12 Shall provide a quarterly report to the Buyer, summarising the actions taken and ongoing monitoring evidence to combat Modern Slavery throughout the Supplier's supply chain. The Buyer reserves the right to request additional information from the Supplier to evidence Modern Slavery measures implemented.

6. Income Security

6.1 The Supplier shall:

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

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

6.1.3 All workers shall be provided with written and understandable Information about their employment conditions in respect to wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

6.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

6.1.5 record all disciplinary measures taken against Supplier Staff; and

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

7. Working Hours

7.1 The Supplier shall:

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

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

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

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

7.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 7.3 below.

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

7.3.1 this is allowed by national law;

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

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

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

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

8. Sustainability

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

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

9. Social Value

9.1 **The Supplier shall:**

9.1.1 Support communities and businesses to manage and recover from a global pandemic, through creation of jobs, re-training and improve conditions to promote the physical & mental health of staff recovering from illness;

9.1.2 Create new opportunities in employment for those who face barriers through apprenticeship and training;

9.1.3 Creation of diverse, resilient supply chains through the use of small businesses;

9.1.4 Fight climate change by working towards net zero greenhouse gas emissions;

9.1.5 Provide written evidence upon request from the buyer on what actions and activities have been undertaken to respond to paragraph's 7.1.1 – 7.1.4.

10. PROMPT PAYMENT

10.1 **The Supplier shall:**

10.1.1 Ensure all invoices, for services delivered under this Contract are paid to suppliers in the supply chain within sixty (60) days.

10.1.2 Provide evidence to the Buyer upon request to demonstrate compliance with Paragraph 8.1.1.

Joint Schedule 6 (Key Subcontractors)

11. Restrictions on certain Subcontractors

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

11.2 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.

11.3 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 by completing and submitting a Variation Form as set out in Joint Schedule 2 (Variation Form) and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 11.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 20 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

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

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

11.3.3 the proposed Key Subcontractor employs unfit persons.

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

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

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

11.4.3 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;

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

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

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

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)

1.1 The only processing that the Processor is authorised to do is listed in this Joint Schedule11 by the Controller and may not be determined by the Processor.

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

1.3 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 operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations 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.

1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

(a) process that Personal Data only in accordance with this Joint Schedule 11(Processing Data) unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular this Joint Schedule 11 (Processing 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 clause;

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

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

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

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

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

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

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

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

(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.

1.5 Subject to paragraph 1.6, the Processor shall notify the Controller immediately if it:

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

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

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

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

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

(f) becomes aware of a Data Loss Event.

1.6 The Processor's obligation to notify under paragraph 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

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

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

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

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

(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.

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

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

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

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

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

1.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

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

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause 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 this Contract).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.15 Where the Parties include two or more Joint Controllers as identified in in this Joint Schedule 11 (Processing Data) (in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Annex 2 in replacement of paragraphs 1.1-1.14 for the Personal Data under Joint Control.

Annex 1: a) Authorised Processing Template

Contract:	**Network Services 2 RM3808**
Date:	**1st June 2022**
Description Of Authorised Processing	**Details**
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor in accordance with Clause 14.1 of the Core Terms. In respect of Personal Data under Joint Control, paragraphs 1.1 to 1.14 of Joint Schedule 11 (Processing Data) will not apply and the Parties agree to put in place a Joint Controller Agreement.
Subject matter of the processing	The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide Mobile Voice & Data services to the Buyer.
Duration of the processing	For the duration of the Contract, or longer if required by Law.
Nature and purposes of the processing	The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means).

Type of Personal Data	Name and surname, office address, email address, telephone number, cost centre code.
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), customers/clients, suppliers.
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	The Supplier shall delete and return Personal Data to the Buyer on termination and/or expiry of the Contract unless the Supplier is required by Law to retain the Personal Data. The Buyer will then securely 'destroy' the Personal Data in accordance with its relevant retention and destruction processes.

Annex 1: b) Framework Contract Authorised Processing

Framework Contract	**Network Services 2 RM3808**
Date:	**1st June 2022**
Description Of Authorised Processing	**Details**
Identity of the Controller and the Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, CCS is the Controller and the Supplier is the Processor in accordance with Clause 14.1 of the Core Terms.
Subject matter of the processing	Management of the Network Services 2 Framework Contract between CCS and the Supplier
Duration of the processing	Up to ten (10) years after the expiry or termination of the Framework Contract
Nature and purposes of the processing	To facilitate the fulfilment of the Supplier's obligations arising under this Framework Contract including i. Ensuring effective communication between the Supplier and CCS; and ii. Maintaining full and accurate records of every Call-Off Contract arising under the Framework Contract in accordance with Core Terms Clause 15 (Record Keeping and Reporting)
Type of Personal Data	Includes: i. Contact details of, and communications with, CCS staff concerned with management of the Framework Contract; ii. Contact details of, and communications with, Buyer staff concerned with award and

	management of Call-Off Contracts awarded under the Framework Contract; iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract. iv. Contact details, and communications with Supplier staff concerned with management of the Framework Contract.
Categories of Data Subject	Includes: i. CCS staff concerned with management of the Framework Contract; ii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract; iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract; iv. Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Contract.
Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	All relevant data to be deleted 7 years after the expiry or termination of this Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder

Call-Off Schedule 1 (Transparency Reports)

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

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

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

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

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
[redacted]	[redacted]	To be agreed jointly between Buyer and Supplier following contract signature.	Monthly
[redacted]	[redacted]	To be agreed jointly between Buyer and Supplier following contract signature.	Monthly
[redacted]	[redacted]	To be agreed jointly between Buyer and Supplier following contract signature.	Monthly

Call-Off Schedule 3 (Continuous Improvement)

12. BUYER'S RIGHTS

12.1 This Schedule shall apply only when so specified by a Buyer that has undertaken a Further Competition. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

13. SUPPLIER'S OBLIGATIONS

13.1 The Supplier shall have an on-going obligation throughout the Call-Off Contract Period to identify new or potential improvements to the provision of the Services in accordance with this Call-Off Schedule 3 with a view to reducing the Buyer's costs (including the Call-Off Contract Charges) and/or improving the quality and efficiency of the Services and their supply to the Buyer. As part of this obligation the Supplier shall identify and report to the Buyer once every twelve (12) months regarding:

13.1.1 the emergence of new and evolving relevant technologies which could improve the ICT Environment and/or the provision of the Services, and those technological advances potentially available to the Supplier and the Buyer which the Parties may wish to adopt;

13.1.2 new or potential improvements to the Services or the provision of the Services including in respect of the quality, responsiveness, procedures, benchmarking methods, ways of performing the Services and customer support services in relation to the Services;

13.1.3 changes in business processes and working practices that would enable the Services to be provided at lower cost and/or with greater benefits to the Buyer;

13.1.4 changes to the ICT Environment, business processes and working practices that would enable reductions in the total energy consumed in the provision of the Services;

13.1.5 improvements which the Supplier uses or is planning to use with its other customers;

13.1.6 proposals as to how any investment required for continuous improvement could be shared with other customers of the Supplier;

13.1.7 a zero usage report for the delivered Services;

measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives; and

13.1.8 any variation in Charges and cost / benefit analysis of the potential improvements identified subject to this Call-Off Schedule 3.

13.2 The Supplier shall ensure that the information that it provides to the Buyer shall be sufficient for the Buyer to decide whether any improvement should

be implemented. The Supplier shall provide any further information that the Buyer requests.

13.3 If the Buyer wishes to incorporate any improvement identified by the Supplier, including any impact on the Charges declared by the Supplier as part of that improvement, the Buyer shall request a Variation in accordance with the Variation Procedure.

13.4 Notwithstanding anything to the contrary in this Call-Off Contract, the Parties may not change or improve the Services in any way which adversely affects or may adversely affect any relevant PSN Standards or HSCN obligations and processes.

Call-Off Schedule 5 (Pricing Details)

1. CHARGES

1.1 The price for the implementation and ongoing associated services, detailed in Annex A below, is: £300,561.60 ex VAT.

2. INVOICING

2.1 The Supplier will invoice the Buyer for Mobile Voice & Data services.

2.2 The Supplier will submit electronic invoices to the Buyer for Services monthly in arrears.

2.3 The Supplier will provide all invoicing and billing no later than four (4) months after the Services were delivered. The Buyer has the ability to approve or reject all invoices within 10 working days. All invoices presented to the Buyer for Services delivered more than four (4) months before provision of the invoice shall be invalid and the Buyer shall have no obligation or liability in respect of such invoices

2.4 The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.

2.5 The Supplier will provide supporting itemised management information in a format suitable to the Buyer at the end of each Service Management Period.

2.5 Invoices will be sent to [redacted]. In addition, an electronic invoice will be sent to: [redacted].

3. ASSUMPTIONS

3.1 The Buyer acknowledges that the total Charges, approach and timescale are based on the following Assumptions and Parameters: Tariff Migration only. No replacement SIMs required. No device roll-out required.

3.2 In the event that any one or more of the Assumptions set out in paragraph 3.1 proves to be incorrect or where they change then the parties shall work together (acting reasonably and in good faith) to reduce the impact of this within the agreed timescales and estimated Charges and failing that then either:

3.2.1 The parties shall agree a contract variation, as per joint schedule 2 – variation form, to deal with the impact; or

3.2.2 The matter shall be referred to the Dispute Resolution Procedure.

Annex A – Pricing Schedules

The volumes given are for evaluation purposes only and are not the final contractual, which will vary depending on the Buyer's need.

Scenario 1 – All inclusive UK Voice and SMS

Item	Per Month Cost (ex VAT)	Number of months	Total (ex VAT)
[redacted]	[redacted]	[redacted]	[redacted]

*Out of Bundle**

Scenario 2 – Shared Data Bundle

Item	Per Month Cost (ex VAT)	Number of months	Total (ex VAT)
[redacted]	[redacted]	[redacted]	[redacted]

*Out of Bundle***

Scenario 3 – Transferable Data Management Licenses (optional service)

Item	Per Month Cost (ex VAT)	Number of months	Total (ex VAT)
[redacted]	[redacted]	[redacted]	[redacted]

Total Price: £300,561.60 ex VAT

[redacted]

[redacted]**Additional Non-Scored Pricing Information**

Implementation Costs

Description	Cost (ex VAT)
[redacted]	[redacted]

Training Costs

Description	Cost (ex VAT)
[redacted]	[redacted]

Additional Services Costs (any other costs that may be payable to deliver your offering)

Description
[redacted]

[redacted]

Call-Off Schedule 6 (ICT Services)

1. Definitions

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

"Buyer Property"	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Commercial off the shelf Software" or "COTS Software"	non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms;
"Core Network"	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract;
"Defect"	any of the following: a) any error, damage or defect in the manufacturing of a Deliverable; or b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or

	the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;
"Emergency Maintenance"	ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;
"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Subcontractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;
"Maintenance Schedule"	has the meaning given to it in paragraph 8 of this Schedule;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"New Release"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;

"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or c) where any part of the Supplier System is situated;
"Permitted Maintenance"	has the meaning given to it in paragraph 8.2 of this Schedule;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software COTS Software and non-COTS Supplier and third party software;
"Software Supporting Materials"	has the meaning given to it in paragraph 9.1 of this Schedule;
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;

"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Subcontractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

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

3. Buyer due diligence requirements

3.1. This paragraph 3 applies where the Buyer has conducted a Further Competition Procedure. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

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

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

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

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

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

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

3.2.2. each aspect, if any, of the Operating Environment where the provision of the Services will be subject to site surveys, wayleaves and/or any other consents not yet granted;

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

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

4. Software warranty

4.1. The Supplier represents and warrants that:

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

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and

4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

5.1. The Supplier shall:

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

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

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

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

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

6. Standards and Quality Requirements

6.1. The Supplier shall where requested by the Buyer as part of their Further Competition Procedure, and within the timescales specified by the Buyer, develop, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN

ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**")**.**

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

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

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

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

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

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

7. ICT Audit

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

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

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

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

8. Maintenance of the ICT Environment

8.1. The Supplier shall where requested by the Buyer as part of their Further Competition Procedure, create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (other than to the Core Network) (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance, including to the Core Network.

8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that

the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Supplier: Specially Written Software

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

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

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

9.1.2. The Supplier shall:

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

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

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

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

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

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

b) third party software that is not COTS Software

9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use, adapt, and sub-license the same

for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call-Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

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

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

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

9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.2 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days

after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

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

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

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

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

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

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

9.3.4.2. will no longer be made commercially available.

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

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

9.4.1.1. a Central Government Body; or

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

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

9.5. **Licence granted by the Buyer**

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

9.6. **Open Source Publication**

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

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

9.6.1.2. based on Open Standards (where applicable),

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

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

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

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

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

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

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

9.6.2.6. do not contain any Malicious Software.

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

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

9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on

such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. **Malicious Software**

9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. Supplier-Furnished Terms

10.1. Software Licence Terms

10.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in Part 1A of Call-Off Schedule 21.

10.1.2. Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in Part 1B of Call-Off Schedule 21.

11. CUSTOMER PREMISES

11.1 Licence to occupy Buyer Premises

11.1.1 Any Buyer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this Call-Off Contract. The Supplier shall have the use of such Buyer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or

abandonment of this Call-Off Contract and in accordance with Call-Off Schedule 10 (Exit Management).

11.1.2 The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Call-Off Contract and the Supplier shall co-operate (and ensure that the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.

11.1.3 Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of this Call-Off Schedule 6 and set out in the Order Form (or elsewhere in this Call-Off Contract), should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any modification work which it approves pursuant to this paragraph 11.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

11.1.4 The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.

11.1.5 The Parties agree that there is no intention on the part of the Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to this Call-Off Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

11.2 Security of Buyer Premises

11.2.1 The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.

11.2.2 The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

12. Buyer Property

12.1 Where the Buyer issues Buyer Property free of charge to the Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.

12.2 The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.

12.3 The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Subcontractors and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.

12.4 The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.

12.5 The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with this Call-Off Contract and for no other purpose without Approval.

12.6 The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance with Call-Off Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.

12.7 The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and tear), unless such loss or damage was solely caused by an Authority Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

13. Supplier Equipment

13.1 Unless otherwise stated in the Order Form (or elsewhere in this Call-Off Contract), the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

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

13.3 The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Call-Off Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

13.4 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

13.5 Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Call Off Contract, including the Service Levels.

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

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

13.7.1 remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with this Call-Off Contract; and

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

Call-Off Schedule 7 (Key Supplier Staff)

13.1 1.1 The Annex 1 to this Schedule lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles ("**Key Staff**") at the Start Date.

13.2 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

13.3 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.

13.4 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.

13.5 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 30 days notice;

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

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

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

Annex 1- Key Roles

Key Role	Key Staff	Contract Details
Customer Services Team Leader	[redacted]	[redacted]
Customer Services Senior Team Leader	[redacted]	[redacted]
Senior Sales Manager	[redacted]	[redacted]
Channel Sales Director	[redacted]	[redacted]
Sales Executive	[redacted]	[redacted]
Service Advisor – Off-Site LITE	TBC	TBC

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

PART B: BESPOKE BCDR PLAN

14. Introduction

14.1 The following paragraphs 2 to 10 shall apply where the Buyer has as part of a Further Competition required that the Supplier provides a bespoke BCDR Plan.

15. Definitions

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

"BCDR Plan"	has the meaning given to it in Paragraph 3.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 16.3.2 of this Schedule;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 16.3.3 of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph 20.2 of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph 20.3 of this Schedule;

16. BCDR Plan

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

16.2 The Supplier shall prepare and deliver to the Buyer, for the Buyer's written approval, a plan within 3 months of the contract Start Date, which shall detail the processes and arrangements that the Supplier shall follow to:

16.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

16.2.2 the recovery of the Deliverables in the event of a Disaster.

16.3 The BCDR Plan shall be divided into three sections:

16.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;

16.3.2 Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

16.3.3 Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

16.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

17. General Principles of the BCDR Plan (Section 1)

17.1 Section 1 of the BCDR Plan shall:

17.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

17.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

17.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

17.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;

17.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

17.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

17.1.7 provide for documentation of processes, including business processes, and procedures;

17.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

17.1.9 identify the procedures for reverting to "normal service";

17.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

17.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

17.1.12 provide for the provision of technical assistance to key contacts at the Buyer as reasonably required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

17.2 The BCDR Plan shall be designed so as to ensure that:

17.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

17.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

17.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

17.2.4 it details a process for the management of disaster recovery testing.

17.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

17.4 The Supplier shall not be entitled to any relief from its obligations under the Service Levels or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

18. Business Continuity (Section 2)

18.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

18.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

18.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

18.2 The Business Continuity Plan shall:

18.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;

18.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

18.2.3 specify any applicable Service Levels with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

18.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

19. Disaster Recovery (Section 3)

19.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

19.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

19.2.1 loss of access to the Buyer Premises;

19.2.2 loss of utilities to the Buyer Premises;

19.2.3 loss of the Supplier's helpdesk;

19.2.4 loss of a Subcontractor;

19.2.5 emergency notification and escalation process;

19.2.6 contact lists;

19.2.7 staff training and awareness;

19.2.8 BCDR Plan testing;

19.2.9 post implementation review process;

19.2.10 any applicable Service Levels with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

19.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

19.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

19.2.13 testing and management arrangements.

20. Review and changing the BCDR Plan

20.1 The Supplier shall review the BCDR Plan:

20.1.1 on a regular basis and as a minimum once every six (6) Months;

20.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 9; and

20.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 20.1.1 and 20.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

20.2 Each review of the BCDR Plan pursuant to Paragraph 20.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

20.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

20.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

20.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or

procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

21. Testing the BCDR Plan

21.1 The Supplier shall test the BCDR Plan:

21.1.1 regularly and in any event not less than once in every Contract Year;

21.1.2 in the event of any major reconfiguration of the Deliverables;

21.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).

21.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

21.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

21.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

21.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

21.5.1 the outcome of the test;

21.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

21.5.3 the Supplier's proposals for remedying any such failures.

21.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

22. Invoking the BCDR Plan

22.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

23. Circumstances beyond your control

23.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

PART B: ANNEX 1 Bespoke BCDR Plan

[redacted]

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

24. Definitions

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

"Breach of Security"	the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.

25. Complying with security requirements and updates to them

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

25.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

25.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

25.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

25.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

26. Security Standards

26.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

26.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

26.2.1 is in accordance with the Law and this Contract;

26.2.2 as a minimum demonstrates Good Industry Practice;

26.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

26.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

26.3 The references to standards, guidance and policies contained or set out in Paragraph 26.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

26.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

27. Security Management Plan

27.1 Introduction

27.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

27.2 Content of the Security Management Plan

27.2.1 The Security Management Plan shall:

(a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

(b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

(c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

(d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

(e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

(f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

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

27.3 **Development of the Security Management Plan**

27.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 27.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

27.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 27.3.1, or any subsequent revision to it in accordance with Paragraph 27.4, is Approved it will be adopted immediately and will replace the previous version of the Security

Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

27.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 27.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 27.2 shall be deemed to be reasonable.

27.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 27.3.2 or of any change to the Security Management Plan in accordance with Paragraph 27.4 shall not relieve the Supplier of its obligations under this Schedule.

27.4 **Amendment of the Security Management Plan**

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

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Deliverables and/or associated processes;

(c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

(d) any new perceived or changed security threats; and

(e) any reasonable change in requirements requested by the Buyer.

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

(a) suggested improvements to the effectiveness of the Security Management Plan;

(b) updates to the risk assessments; and

(c) suggested improvements in measuring the effectiveness of controls.

27.4.3 Subject to Paragraph 27.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 27.4.1, a

request by the Buyer or otherwise) shall be subject to the Variation Procedure.

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

28. Security breach

28.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

28.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 28.1, the Supplier shall:

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

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

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

(c) prevent an equivalent breach in the future exploiting the same cause failure; and

(d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

28.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Appendix A: Departmental Security Requirements

1. Departmental Security Standards for Business Services and ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	means the Government's HMG Baseline Personal Security Standard . Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" "Certified Cyber Security Consultancy"	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" "Certified Professional"	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"CPA" "Commercial Product Assurance" [formerly called "CESG Product Assurance"]	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body
"Data" "Data Controller" "Data Protection Officer" "Data Processor" "Personal Data" "Personal Data requiring Sensitive Processing" "Data Subject", "Process" and "Processing"	shall have the meanings given to those terms by the Data Protection Act 2018

"Department's Data" "Department's Information"	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
"DfE" "Department"	means the Department for Education
"Departmental Security Standards"	means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.
"Digital Marketplace / G-Cloud"	means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
End User Devices	means the personal computer or consumer devices that store or process information.
"Good Industry Practice" "Industry Good Practice"	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"Good Industry Standard" "Industry Good Standard"	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"GSC" "GSCP"	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	means Her Majesty's Government
"ICT"	means Information and Communications Technology (ICT) and is used as an extended

	synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
"ISO/IEC 27001" "ISO 27001"	is the International Standard for Information Security Management Systems Requirements
"ISO/IEC 27002" "ISO 27002"	is the International Standard describing the Code of Practice for Information Security Controls.
"ISO 22301"	is the International Standard describing for Business Continuity
"IT Security Health Check (ITSHC)" "IT Health Check (ITHC)" "Penetration Testing"	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
"Need-to-Know"	means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.
"NCSC"	The National Cyber Security Centre (NCSC) is the UK government's National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
"OFFICIAL" "OFFICIAL-SENSITIVE"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP). the term 'OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.
"RBAC" "Role Based Access Control"	means Role Based Access Control. A method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Storage Area Network" "SAN"	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
"Secure Sanitisation"	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.

	NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"Senior Information Risk Owner" "SIRO"	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
"SPF" "HMG Security Policy Framework"	means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework

1.1. The Contractor shall be aware of and comply the relevant HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

– (Guidance: Providers on the HMG Digital Marketplace / GCloud that have demonstrated compliance, as part of their scheme application, to the relevant scheme's security framework, such as the HMG Cloud Security Principles for the HMG Digital Marketplace / GCloud, may on presentation of suitable evidence of compliance be excused from compliance to similar clauses within the DfE Security Clauses detailed in this section (Section 12).)

1.2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

– (Guidance: Details of the acceptable forms of equivalence are stated at Section 9 of Annex A within the link to Cabinet Office document in this clause).

– (Guidance: The Department's expectation is that the certification scope will be relevant to the services supplied to, or on behalf of, the Department. However, where a contractor or (sub) contractor is able to evidence a valid exception or certification to an equivalent recognised scheme or standard, such as ISO 27001, then certification under the Cyber Essentials scheme could be waived. Changes to the Cabinet Office Action Note will be tracked by the DfE)

– (Guidance: The department's expectation is that SMEs or organisations of comparable size shall be expected to attain and maintain Cyber Essentials. Larger organisations or enterprises shall be expected to attain and maintain Cyber Essentials Plus.)

1.3 Where clause 12.2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

– (Guidance: The Department's expectation is that suppliers claiming certification to ISO/IEC 27001 shall provide the Department with copies of their Scope of Certification, Statement of Applicability and a valid ISO/IEC 27001 Certificate issued by an authorised certification body. Where the provider is able to provide a valid Cyber Essentials certification then certification under the ISO/IEC 27001 scheme could be waived and this clause may be removed.)

1.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service and will handle all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

– (Guidance: The Department's expectations are that all contractors shall handle the Department's information in a manner compliant with the GSCP. Details of the GSCP can be found on the GOV.UK website at: https://www.gov.uk/government/publications/government-security-classifications.)

– (Guidance: Compliance with the GCSP removes the requirement for the department to issue a Security Aspects Letter (SAL) to the contractor).

1.5 Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required in line with clause 12.14.

– (Guidance: Advice on HMG secure sanitisation policy and approved methods are described at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

1.6 The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

– (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

1.7 The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Departmental Data or systems shall be considered to be sensitive data and must be protected accordingly.

– (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

1.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:

- physical security controls;
- good industry standard policies and processes;
- malware protection;
- boundary access controls including firewalls, application gateways, etc;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- use of secure device configuration and builds;
- software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- user identity and access controls, and, including the use of multi-factor authentication for sensitive data and privileged account accesses;
- any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
    - retained and protected from tampering for a minimum period of six months;
    - made available to the department on request.

– (Guidance: Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources or locations managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

– (Guidance: The Minimum Cyber Security Standard issued by Cabinet Office and Information Commissioner's Office advice for the protection of sensitive and personal information recommends the use of Multi-Factor Authentication (MFA). The MFA implementation must have two factors as a minimum; with the second factor being facilitated through a separate and discrete channel, such as, a secure web page, voice call, text message or via a purpose built mobile app, such as; Microsoft Authenticator.)

– (Guidance: Further advice on appropriate levels of security audit and log collection to be applied can be found at: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring.)

1.9 The contractor shall ensure that any departmental data (including email) 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.

1.10 The contractor shall ensure that any departmental 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 department except where the department has given its prior written consent to an alternative arrangement.

(Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the use of removable media as described in this clause is either prohibited or not required in order to deliver the service this clause shall be revised as follows: - 'The use of removable media in any form is not permitted'.)

1.11 The contractor shall ensure that any device which is used to process departmental 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 and https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

– (Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

1.12 Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

– (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: https://www.cpni.gov.uk/secure-destruction)

1.13 When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

1.14 In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.

– (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning sanitisation must be in accordance with guidance provided by NCSC and CPNI.

1.15 In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

– (Guidance: Where there is no acceptable secure sanitisation method available for a piece of equipment, or it is not possible to sanitise the equipment due to an irrecoverable technical defect, the storage media involved shall be destroyed using an HMG approved method described at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.)

– (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: https://www.cpni.gov.uk/secure-destruction)

– (Guidance: The term ‘accounted for’ means that assets and documents retained, disposed of or destroyed should be listed and provided to the department as proof of compliance to this clause.)

1.16 Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.

– (Guidance: Further details of the requirements for HMG BPSS clearance are available on the website at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard)

– (Guidance: Further details of the requirements for National Security Vetting, if deemed necessary for this contract are available at: https://www.gov.uk/government/publications/hmg-personnel-security-controls)

1.17 All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.

1.18 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

– (Guidance: The business continuity and disaster recovery plans should be aligned with industry good practice and it is the Department’s expectation that all vendors providing services or infrastructure to the Department will have plans that are aligned to the ISO 22301 standard in place. Further information on the requirements of ISO 22301 may be found in the standard.)

1.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data, including user credentials, used or handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.

Incidents shall be reported through the department's nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

1.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

– (Guidance: Further information on IT Health Checks and the NCSC CHECK Scheme which enables penetration testing by NCSC approved companies can be found on the NCSC website at: https://www.ncsc.gov.uk/scheme/penetration-testing.)

1.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.

– (Guidance: The offshoring of HMG information outside of the UK is subject to approval by the Departmental SIRO).

1.22 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors', compliance with the clauses contained in this Section.

1.23 The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

– (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning their organisation. Further advice and guidance on the Department's security assurance processes can be supplied on request. Information about the HMG Supplier Assurance Framework can be found at: https://www.gov.uk/government/publications/government-supplier-assurance-framework

– (Guidance: Further information on the CCP and CCSC roles described above can be found on the NCSC website at: https://www.ncsc.gov.uk/information/about-certified-professional-scheme and https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy)

1.24 Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:

- Compliance with HMG Minimum Cyber Security Standard.
- Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
- Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.

- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

1.25 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

Annex 1: Baseline security requirements

29. Handling Classified information

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

2. End user devices

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

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

3. Data Processing, Storage, Management and Destruction

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

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

3.3 The Supplier shall:

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

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

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

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

4. Ensuring secure communications

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

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

5. Security by design

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

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

6. Security of Supplier Staff

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

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

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

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

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

7. Restricting and monitoring access

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

8. Audit

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

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

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

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

8.1.4 The Supplier shall retain audit records collected in compliance with this Paragraph 0 for a period of at least 6 Months.

Call-Off Schedule 10 (Exit Management)

30. Definitions

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

"Core Network"	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract;
"Core Network Assets"	the assets used in the provision of the Core Network;
"Exclusive Assets"	Supplier Assets used exclusively by the Supplier [or a Key Subcontractor] in the provision of the Deliverables;
"Exit Information"	has the meaning given to it in Paragraph 32.1 of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under this Schedule;
"Net Book Value"	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier [or a Key Subcontractor] in connection with the Deliverables but which are also used by the Supplier [or Key Subcontractor] for other purposes excluding the Core Network Assets;
"Registers"	the register and configuration database referred to in Paragraph 31.2 of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether

	those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those services are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	a) the provision of any configuration information reasonably required to effect the implementation of the Replacement Services excluding the Core Network; b) any activity required to facilitate the transition from the live operation of an existing Service to the live operation of a Replacement Service excluding the Core Network; and c) the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in Paragraph 34.1 of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 34.2 of this Schedule;
"Transferable Assets"	Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation, excluding such contracts relating to the Core Network;
"Transferring Assets"	has the meaning given to it in Paragraph 37.2.1 of this Schedule;

"Transferring Contracts"	has the meaning given to it in Paragraph 37.2.3 of this Schedule.

31. Supplier must always be prepared for contract exit

31.1 The Supplier shall, if applicable, within thirty (30) days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

31.2 During the Contract Period, the Supplier shall promptly:

31.2.1 create and maintain a detailed register of i) all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and ii) Sub-contracts and other relevant agreements required in connection with the Deliverables insofar as they relate to Exclusive Assets and Non-Exclusive Assets; and

31.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables (excluding the Core Network) ("**Registers**").

31.3 The Supplier shall:

31.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

31.3.2 procure that all licences for Third Party Software, and all Sub-Contracts, in relation to Exclusive and Non-Exclusive Assets shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

31.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

31.5 For the avoidance of doubt, the Supplier shall only be required to provide details of all assets as described in Section 2.2 and 2.3 of this Schedule, if such assets are provided as part of the services under this agreement.

32. Assisting re-competition for Deliverables

32.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to

tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

32.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

32.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information (excluding the Core Network) which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

32.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables (excluding the Core Network); and not be disadvantaged in any procurement process compared to the Supplier.

33. Exit Plan

33.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 33.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

33.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 33.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

33.3 The Exit Plan shall set out, as a minimum:

33.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

33.3.2 how the Deliverables (excluding the Core Network) will transfer to the Replacement Supplier and/or the Buyer;

33.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

33.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

33.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

33.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

33.3.7 proposals for the identification and return of all Buyer Assets in the possession of and/or control of the Supplier or any third party;

33.3.8 proposals for the disposal of any redundant Deliverables and materials;

33.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

33.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

33.4 The Supplier shall:

33.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) every twelve (12) months throughout the Contract Period; and

(b) no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

33.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

33.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 33.2 or 33.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

33.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

34. Termination Assistance

34.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least one (1) Month prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

34.1.1 the nature of the Termination Assistance required;

34.1.2 the start date and period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the date that the Supplier ceases to provide the Deliverables; and

34.1.3 whether the Buyer requires any additional services to assist with exit beyond what is required by this Schedule, which may be chargeable by the Supplier.

34.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the Termination Assistance Notice period provided that such extension shall not extend for more than six (6) Months beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier of such this extension no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than twenty (20) Working Days' written notice upon the Supplier.

34.3 Where the Buyer indicates in a Termination Assistance Notice that it requires any additional services to assist with exit in accordance with paragraph 5.1.3, the Supplier shall provide to the Buyer within ten (10) Working Days of receipt of such Termination Assistance Notice a quotation in the form of an itemised list of costs (in line with any day rates specified in the Contract) for each line of the additional services that the Buyer requires. Within five (5) Working Days of receipt of such quotation the Buyer shall confirm to the Supplier which of those itemised services it requires and the Supplier shall provide those services as part of the Termination Assistance at the Charges provided in the quotation.

34.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

35. Termination Assistance Period

35.1 Throughout the Termination Assistance Period the Supplier shall:

35.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

35.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

35.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

35.1.4 subject to Paragraph 35.3, provide the Deliverables and the Termination Assistance at no detriment to the Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

35.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

35.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

35.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 35.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

35.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

36. Obligations when the contract is terminated

36.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

36.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

36.2.1 vacate any Buyer Premises;

36.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

36.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

36.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

37. Assets, Sub-contracts and Software

37.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

37.1.1 terminate, enter into or vary any Sub-contract insofar as it relates to Exclusive Assets and Non-Exclusive Assets:; or

37.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets; or

37.1.3 terminate, enter into or vary any licence for any software in connection with the Deliverables excluding the Core Network.

37.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

37.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

37.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

37.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**), in order for the Buyer and/or its Replacement Supplier to provide the Deliverables excluding the Core Network from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide:

i) the Deliverables (excluding the Core Network); or

ii) the Replacement Goods and/or Replacement Services (excluding the Core Network).

37.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

37.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

37.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

37.5.1 procure a non-exclusive, perpetual, royalty-free licence (or a licence on such other terms that the Buyer may agree) for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

37.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

37.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

37.7 The Buyer shall:

37.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

37.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

37.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

37.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 37.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 37.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

38. No charges

38.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

39. Dividing the bills

39.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

39.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

39.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

39.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

RM3808 Call-Off Schedule 11 (Installation Works)

1. When this Schedule should be used

1.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision Deliverables requiring installation by the Supplier.

2. How things must be installed

2.1. Where the Supplier reasonably believes, it has completed the Installation Works it shall notify the Buyer in writing. Following receipt of such notice, the Buyer shall inspect the Installation Works and shall, by giving written notice to the Supplier:

2.1.1. accept the Installation Works, or

2.1.2. reject the Installation Works and provide reasons to the Supplier if, in the Buyer's reasonable opinion, the Installation Works do not meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract).

2.2. If the Buyer rejects the Installation Works in accordance with Paragraph reject the Installation Works and provide reasons to the Supplier if, in the Buyer's reasonable opinion, the Installation Works do not meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract)., the Supplier shall immediately rectify or remedy any defects and if, in the Buyer's reasonable opinion, the Installation Works do not, within five (5) Working Days of such rectification or remedy, meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract), the Buyer may terminate this Contract for material Default.

2.3. The Installation Works shall be deemed to be completed when the Supplier receives a notice issued by the Buyer in accordance with Paragraph accept the Installation Works, or. Notwithstanding the acceptance of any Installation Works in accordance with Paragraph 2.2, the Supplier shall remain solely responsible for ensuring that the Goods and the Installation Works conform to the specification in the Call-Off Order Form (or elsewhere in this Contract). No rights of estoppel or waiver shall arise as a result of the acceptance by the Buyer of the Installation Works.

2.4. Throughout the Contract Period, the Supplier shall have at all times all licences, approvals and consents necessary to enable the Supplier and the Supplier Staff to carry out the Installation Works.

Call-Off Schedule 13 (Implementation Plan and Testing)

PART A - Implementation

40. Definitions

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

"Delay"	a) a delay in the Achievement of a Milestone by its Milestone Date; or b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
"Milestone Payment"	a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;

41. Agreeing and following the Implementation Plan

41.1 Part A of this Schedule shall only apply if specified by a Buyer that has undertaken a Further Competition.

41.2 A draft of the Implementation Plan is set out in the Annex to Part A of this Schedule. The Supplier shall provide a further draft Implementation Plan 10 days after the Call-Off Contract Start Date.

41.3 The draft Implementation Plan:

41.3.1 must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and

41.3.2 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

41.4 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days

of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

41.5 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

41.6 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

42. Reviewing and changing the Implementation Plan

42.1 Subject to Paragraph 42.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.

42.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

42.3 Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

42.4 Where the Supplier is responsible for the failure to Achieve a Milestone by the relevant Milestone Date this shall constitute a material Default.

43. Security requirements before the Start Date

43.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.

43.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

43.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

43.4 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be

responsible for meeting the costs associated with the provision of security cleared escort services.

43.5 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

44. What to do if there is a Delay

44.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

44.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

44.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

44.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and

44.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

45. Compensation for a Delay

45.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

45.1.1 the Supplier acknowledges and agrees that any Delay Payment 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 Achieve the corresponding Milestone;

45.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:

(a) the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

(b) the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

45.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

45.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

45.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

PART A Annex 1: Implementation Plan

The Implementation Plan is set out below and the Milestones to be Achieved are identified below. Milestone dates below are indicative. Final dates will be agreed prior to contract signature

Milestone	Deliverable Items	Duration	Milestone Date	Buyer Responsibilities	Milestone Payments	Delay Payments
1	Detailed Implementation Plan	10 working days	TBC	Sign off of final plan	£0	£0
2	Tariff Build	5 working days	TBC	UAT success.	£0	£0
3	End User Training	20 working days	TBC		£0	£0
3	Go-Live	TBC	TBC	Sign off	£0	£ TBC (15% of total milestone costs)

The Milestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing)

For the purposes of Paragraph 45.1.2 the Delay Period Limit shall be no longer than 1 month after the scheduled completion date of the Go-Live milestone above.

Part B: Testing

46. Definitions

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

"Component"	any constituent parts of the Deliverables;
"Material Test Issue"	a Test Issue of Severity Level 1 or Severity Level 2;
"Satisfaction Certificate"	a certificate materially in the form of the document contained in Annex 2 of Part B of this Schedule issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;
"Severity Level"	the level of severity of a Test Issue, the criteria for which are described in Annex 1 of Part B of this Schedule;
"Test Issue Management Log"	a log for the recording of Test Issues as described further in Paragraph 53.1 of Part B of this Schedule;
"Test Issue Threshold"	in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Reports"	the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of Part B of this Schedule;
“Test Strategy”	a strategy for the conduct of Testing as described further in Paragraph 48.2 of Part B of this Schedule;
“Test Success Criteria”	in relation to a Test, the test success criteria for that Test as referred to in

	Paragraph 50 of Part B of this Schedule;
"Test Witness"	any person appointed by the Buyer pursuant to Paragraph 54 of Part B of this Schedule; and
"Testing Procedures"	the applicable testing procedures and Test Success Criteria set out in this Schedule.

47. How testing should work

47.1 Part B of this Schedule shall only apply if specified by a Buyer that has undertaken a Further Competition.

47.2 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.

47.3 The Supplier shall not submit any Deliverable for Testing:

47.3.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

47.3.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and

47.3.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

47.4 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

47.5 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

48. Planning for testing

48.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.

48.2 The final Test Strategy shall include:

48.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;

48.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

48.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;

48.2.4 the procedure to be followed to sign off each Test;

48.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;

48.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;

48.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;

48.2.8 the technical environments required to support the Tests; and

48.2.9 the procedure for managing the configuration of the Test environments.

49. Preparing for Testing

49.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.

49.2 Each Test Plan shall include as a minimum:

49.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and

49.2.2 a detailed procedure for the Tests to be carried out.

49.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

50. Passing Testing

50.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 49.

51. How Deliverables will be tested

51.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least ten (10) Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).

51.2 Each Test Specification shall include as a minimum:

51.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

51.2.2 a plan to make the resources available for Testing;

51.2.3 Test scripts;

51.2.4 Test pre-requisites and the mechanism for measuring them; and

51.2.5 expected Test results, including:

(a) a mechanism to be used to capture and record Test results; and

(b) a method to process the Test results to establish their content.

52. Performing the tests

52.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

52.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 54.3.

52.3 The Supplier shall notify the Buyer at least ten (10) Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.

52.4 The Buyer may raise and close Test Issues during the Test witnessing process.

52.5 The Supplier shall provide to the Buyer in relation to each Test:

52.5.1 a draft Test Report not less than two (2) Working Days prior to the date on which the Test is planned to end; and

52.5.2 the final Test Report within five (5) Working Days of completion of Testing.

52.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

52.6.1 an overview of the Testing conducted;

52.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;

52.6.3 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

52.6.4 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 53.1; and

52.6.5 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

52.7 When the Supplier has completed a Milestone it shall submit any Deliverables relating to that Milestone for Testing.

52.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier, any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.

52.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

53. Discovering Problems

53.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

53.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.

53.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

54. Test witnessing

54.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

54.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

54.3 The Test Witnesses:

54.3.1 shall actively review the Test documentation;

54.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

54.3.3 shall not be involved in the execution of any Test;

54.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

54.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

54.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

54.3.7 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

55. Auditing the quality of the test

55.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

55.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

55.3 The Buyer will give the Supplier at least five (5) Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit.

55.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

55.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.

55.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

56. Outcome of the testing

56.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

56.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:

56.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;

56.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

56.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

56.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

56.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:

56.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

56.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.

56.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).

56.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues any other reasons for the relevant Milestone not being Achieved.

56.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.

56.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

56.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to

issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

56.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within ten (10) Working Days of receipt of the Buyer's report pursuant to Paragraph 55.5); and

56.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

57. Risk

57.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:

57.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or

57.1.2 affect the Buyer's right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

PART B Annex 1: Test Issues – Severity Levels

1. Severity 1 Error

1.1 This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

2. Severity 2 Error

2.1 This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:

2.1.1 causes a Component to become unusable;

2.1.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

2.1.3 has an adverse impact on any other Component(s) or any other area of the Deliverables;

3. Severity 3 Error

3.1 This is an error which:

3.1.1 causes a Component to become unusable;

3.1.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

3.1.3 has an impact on any other Component(s) or any other area of the Deliverables;

but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

4. Severity 4 Error

4.1 This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables; and

5. Severity 5 Error

5.1 This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

PART B Annex 2: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

Dear Sirs,

Satisfaction Certificate

Deliverable/Milestone(s): [Insert relevant description of the agreed Deliverables/Milestones].

We refer to the agreement (**"Call-Off Contract"**) [insert Call-Off Contract reference number] relating to the provision of the [insert description of the Deliverables] between the [*insert Buyer name*] (**"Buyer"**) and [*insert Supplier name*] (**"Supplier"**) dated [*insert Call-Off Start Date dd/mm/yyyy*].

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully

[insert Name]

[insert Position]

acting on behalf of [insert name of Buyer]

Call-Off Schedule 14 (Service Levels)

6. Introduction

6.1 The Buyer will specify in the Order Form at Further Competition whether Part A or Part B to this Schedule applies.

6.2 Where the Buyer has not conducted a Further Competition Part B to this Schedule will apply.

7. Definitions

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

"Achieved Service Level"	means the actual level of performance of a Service achieved by the Supplier in relation to a Service Level Performance Criteria for a Service Period;
"Agreed Service Time"	means the period during which the Supplier ensures the Services are Available to the Buyer;
"Available"	a Service shall be "Available" when the Buyer's end users are able to access and use all its functions at a level that enables them to carry out their normal duties. Availability shall be construed accordingly;
"Call-Off Contract Year"	means a consecutive period of twelve (12) Months commencing on the Call-Off Start Date or each anniversary thereof;
"Critical Service Level Failure"	takes the meaning; a) Specified by the Buyer where the Buyer selects Part A to this Call-Off Schedule 14; or b) any instance of critical service level failure specified in Annex 2 to Part B of this Schedule where the Buyer selects Part B to this Schedule;
"Downtime"	means any period of time within the Agreed Service Time during which a Service is not Available, excluding Planned Downtime;
"Imposed Carrier Downtime"	means time during which the Supplier is prevented from supplying the Services due to unavailability of an underlying telecommunications service from a third-party provider on which the Services are dependent. In any instance where the Supplier claims Imposed

	Carrier Downtime, the Supplier must be able to provide evidence to the satisfaction of the Buyer that the interruption to the Services was in fact due in its entirety to unavailability of the underlying service;
"Incident"	means an unplanned incident or interruption to Services, reduction in the quality of the Services or event which could affect the Services in the future;
"Incident Resolution Time"	means the time taken by the Supplier to Resolve an Incident, as set out in this Schedule;
"Planned Downtime"	means the time agreed in advance in writing by the Supplier and Buyer within the Agreed Service Time when a Service is not Available;
"Provisioning"	means the time taken from the placement of an Order for a Service or part thereof until the Service is Available to the Buyer and Provision shall be construed accordingly;
"Resolution"	means an action taken by or on behalf of the Supplier to fully repair the root cause of an Incident or to implement a workaround, such that the Services are returned to being Available. Resolve and Resolved shall be construed accordingly;
"Service Credit Cap"	means: (a) in the period from the Call-Off Start Date to the end of the first Call-Off Contract Year fifteen thousand pounds (£15,000); and (b) during the remainder of the Call-Off Contract Period, thirty five per cent (35%) of the Call-Off Contract Charges payable to the Supplier under this Call-Off Contract in the period of twelve (12) Months immediately preceding the Service Period in respect of which Service Credits are accrued; **unless** otherwise stated in the Order Form during a Further Competition.
"Service Credits"	a) 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; or

b) any service credits specified in the Annex to Part B 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 Desk"	means the single point of contact set up and operated by the Supplier to log, monitor and escalate Incidents, Incident Resolutions and Service Requests;
"Service Failure Threshold"	means the level of performance of a Service which becomes unacceptable to the Buyer, including as set out in each Service Level Performance Criteria and where the Supplier fails to provide the Services in accordance with this Contract;
"Service Level Failure"	means a failure to meet the Service Level Threshold in respect of a Service Level Performance Criterion;
"Service Level Performance Criteria"	means the criteria identified in either; a) Annex 1 to Part A of this Schedule; or b) paragraph 3.6 of Part B of this Schedule, against which the individual metrics are assessed; depending upon whether Part A or Part B is selected by the Buyer
"Service Levels"	means any service levels applicable to the provision of the Services under this Call-Off Contract specified in Call-Off Schedule 14 (Service Levels);
"Service Level Threshold"	shall be as set out against the relevant Service Level Performance Criteria in Annex 1 of Part A, or Annex 1 of Part B, of this Schedule depending upon which option is selected by the Buyer;
"Service Period"	means a recurrent period of one month during the Call-Off Contract Period, unless otherwise specified in the Order Form;
"Unavailable"	in relation to a Service, means that the Service is not Available;

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

8.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Threshold for each Service Level.

8.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A or Part B of this Schedule, as appropriate, 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 Threshold.

8.3 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 C (Performance Monitoring) of this Schedule.

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

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

8.4.2 the Service Level Failure:

(a) exceeds the relevant Service Failure 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

8.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 of the Core Terms (CCS and Buyer Termination Rights).

9. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

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

9.2 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 9 shall be without prejudice to the right of the Buyer to terminate this Contract pursuant to Clause 10.4 of the Core Terms (CCS and Buyer Termination Rights) and/or to claim damages from the Supplier for material Default.

PART B: Long Form Service Levels and Service Credits

1. General provisions

1.1 The Supplier shall provide support and advice, when required by the Buyer, on matters relating to:

1.1.1 Availability of the Services;

1.1.2 quality of the Services;

1.1.3 provisioning;

1.1.4 essential downtime

1.1.5 Buyer support;

1.1.6 complaints handling; and

1.1.7 accurate and timely invoices.

1.2 The Supplier accepts and acknowledges that failure to meet the Service Level Threshold set out in this Part B of this Call-Off Schedule will result in Service Credits being due to the Buyer.

2. Principal points

2.1 The objectives of the Service Levels and Service Credits are to:

2.1.1 incentivise the Supplier to meet the Service Levels and to remedy any failure to meet the Service Levels expeditiously;

2.1.2 ensure that the Services are of a consistently high quality and meet the requirements of the Buyer;

2.1.3 provide a mechanism whereby the Buyer can attain meaningful recognition of inconvenience and/or loss resulting from the Supplier's failure to deliver the level of service for which it has contracted to deliver; and

2.1.4 provide an incentive to the Supplier to comply with and to expeditiously remedy any failure to comply with the Service Levels.

2.2 The Parties acknowledge that:

2.2.1 The Buyer will, in all cases, prefer to receive the Services within the Service Levels in preference to receiving the Service Credits; and

2.2.2 the Supplier shall, in all cases, seek to deliver the Services within the Service Levels in preference to accepting a liability for Service Credits.

3. Service Levels

3.1 The Supplier shall monitor its performance under this Call-Off Contract by reference to the relevant Service Level Performance Criteria for achieving the Service Levels and shall send the Buyer a Performance Monitoring Report detailing the level of service which was achieved in accordance with the provisions of Part C (Performance Monitoring) of this Call-Off Schedule.

3.2 The Supplier shall, at all times, provide the Services in such a manner that the Service Level Thresholds are achieved.

3.3 If the level of performance of the Supplier of any element of the provision by it of the Services during the Call-Off Contract period:

3.3.1 is likely to or fails to meet any Service Level Threshold; or

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

(A) 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; and

(B) If the action taken under paragraph (A) above has not already prevented or remedied the Service Level Failure or Critical Service Level Failure , the Buyer shall be entitled to instruct the Supplier to comply with the Rectification Plan Process; or

(C) If a Service Level Failure has occurred, deduct from the Call-Off Contract Charges the applicable Service Credits payable by the Supplier to the Buyer in accordance with the calculation formula set out in Annex 1 of this Part B of this Call-Off Schedule; or

(D) If a Critical Service Level Failure has occurred, exercise its right to compensation for such non-availability of Services via this Call-Off Contract.

3.4 Approval and implementation by the Buyer of any Rectification Plan shall not relieve the Supplier of any continuing responsibility to achieve the Service Levels, or remedy any failure to do so, and no estoppels or waiver shall arise from any such Approval and/or implementation by the Buyer.

3.5 The Buyer may enhance or otherwise modify the Service Levels required during a Further Competition Procedure.

3.6 The Services are subject to the following four Service Level Performance Criteria as set out in paragraph 6 of this Part B of Call-Off Schedule 14:

3.6.1 Availability;

3.6.2 Incident Resolution;

3.6.3 Quality; and

3.6.4 Provisioning.

4. Agreed Service Time

4.1 The Services will be made Available by the Supplier to the Buyer during the Agreed Service Time.

4.2 The Agreed Service Time applied to the Services will be determined by the Service Maintenance Level selected by the Buyer on the Order Form.

4.3 The Service Maintenance Levels and associated Agreed Service Times is set out in the following table:

Service Maintenance Level	Agreed Service Time
Level 1	Monday – Friday (excluding Bank Holidays) 08:00-18:00
Level 2	Monday – Saturday (excluding Bank Holidays) 08:00-18:00
Level 3	Monday – Sunday (including Bank Holidays) 07:00-21:00
Level 4	Monday – Sunday (including Bank Holidays); 00:00-23:59 (24 hours per day, 7 days per week)

5. Incidents

5.1 If the Services become Unavailable, the Buyer must report the Unavailability as an Incident to the Service Desk.

5.2 Incidents must be classified to one of the following four severity levels:

Severity Level	Description of impact of Incident

Severity 1	The Services are Unavailable across the entire Buyer's estate.
Severity 2	The Services are Unavailable at one of the Buyer's sites.
Severity 3	The Services are Unavailable to an individual user.
Severity 4	All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Buyer or in any other way not attributable to the Supplier.

5.2.1 The Supplier shall manage the Incident to resolution in accordance with this Call-Off Schedule, whilst keeping the Buyer appropriately informed of progress.

6. Service Level Performance Criteria

6.1 Availability

6.1.1 The Supplier shall ensure that the Services are Available during the Agreed Service Time.

6.1.2 Achieved Availability is calculated as a percentage of the total time in a Service Period that the Services should have otherwise been Available to the Buyer using the following formula:

$$\text{Achieved Availability \%} = \frac{(MP - SD) \times 100}{MP}$$

Where:

MP means total time within the Agreed Service Time (excluding Planned Downtime, Imposed Carrier Downtime and any Unavailability attributable to Severity 3 or Severity 4 Incidents) within the relevant Service Period; and

SD means total service downtime within the Agreed Service Time within the relevant Service Period during which a Service and/or part thereof is Unavailable (excluding Planned Downtime, Imposed Carrier Downtime and any Unavailability attributable to Severity 3 or Severity 4 Incidents) within the relevant Service Period.

6.2 Incident Resolution

6.2.1 The Supplier shall ensure that Incidents are resolved within the Maximum Incident Resolution Time.

6.2.2 Maximum Incident Resolution Times are determined by the Severity Levels and Service Maintenance Levels as set out in the following table:

Service Maintenance Level	Severity 1; and Severity 2	Severity 3	Severity 4 (Indicative Only)
Level 1	End of next Working Day	5 Working Days	1 Month
Level 2	End of next Working Day	5 Working Days	1 Month
Level 3	Incident reported by 13:00, resolved same day; reported after 13:00, resolved by 13:00 next Working Day	End of next Working Day	15 Working Days
Level 4	6 hours	End of next Working Day	10 Working Days

6.2.3 Each Incident will either be Resolved within the Maximum Incident Resolution Time, or it will not; and will be reported as such by the Supplier. The time taken to resolve the Incident is not material to this Service Level Performance Criteria.

6.2.4 Achieved Incident Resolution is calculated as a percentage of the total number of Incidents in a Service Period that should have been resolved within the Maximum Incident Resolution Time using the following formula:

$$\text{Achieved Incident Resolution \%} = \frac{(TI - FI) \times 100}{TI}$$

Where:

TI means the total number of Incidents raised by the Buyer during the Service Period (excluding Severity 4 Incidents); and

FI means the total number of Incidents raised by the Buyer during the Service Period that were not resolved within the Maximum Incident Resolution Time (excluding Severity 4 Incidents).

6.2.5 Where an Incident is reported outside the Agreed Service Time, the Incident will be treated as if it has been reported at the beginning of the next Working Day.

6.2.6 The Incident will only be deemed to be Resolved once the Services are Available. However, the Supplier shall not formally close any Incident until the Buyer has confirmed that the Services are Available.

6.3 Quality

6.3.1 The Supplier shall ensure that the Services are delivered of a sufficient quality to meet the provisions of this Call-Off Schedule.

6.3.2 Measurement of answer and response times of the Service Desk will be based on the time taken for the Supplier to respond to the Buyer's call or email. Calls and emails receiving an automated response or calls placed into a queuing system shall be deemed not to have been answered.

6.4 Provisioning

6.4.1 The Services will be provisioned at the outset in accordance with any Implementation Plan and any failure to meet Milestones will be dealt with in accordance with the terms of this Call-Off Contract.

6.4.2 Any delivery of Services or part thereof subsequent to the successful conclusion of the Implementation Plan will be subject to the Service Levels identified in the Variation to this Contract that incorporates those changes; or failing any other agreed Service Level, in accordance with the Supplier's standard provisioning Service Levels.

7. Service Credits

7.1 This section sets out the basic agreed formula used to calculate a Service Credit payable to the Buyer as a result of a Service Level Failure in a given Service Period.

7.2 Service Credit payments are subject to the Service Credit Cap.

7.3 Annex 1 to this Part B of this Call-Off Schedule details the Service Credits available for each Service Level Performance Criterion in the event that the applicable Service Level Threshold is not met by the Supplier.

7.4 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier under Part C (Performance Monitoring) of this Call-Off Schedule to verify the calculation and accuracy of any Service Credits applicable to each Service Period.

7.5 Service Credits are a reduction of the amounts payable in respect of the Services 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 Annex 1 of Part B of this Call-Off Schedule.

7.6 The amount of Service Credit is determined by the tables in Annex 1 of this Part B of Call-Off Schedule 14, using the calculated Achieved Service Level Performance Criteria (e.g. Achieved Availability), the Service Level Threshold and the Service Failure Threshold and is calculated by using the straight line formula below:

Service Credit % = (m*(a-x) + c), where

a is the Service Level Threshold (%) below which Service Credits become payable;

b is the Service Failure Threshold (%);

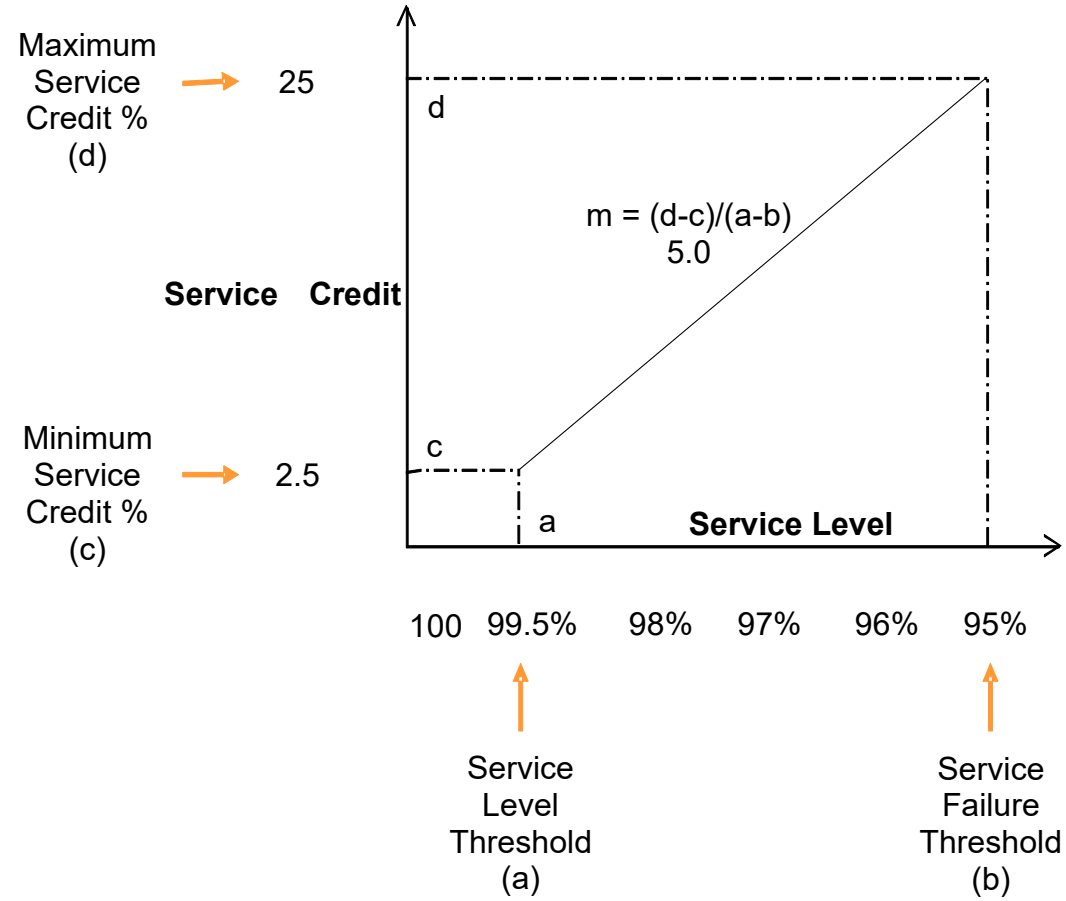
x is the Achieved Service Level Performance Criteria (%) for a Service Period;

c is the minimum Service Credit (%) payable if the Achieved Service Level falls below the Service Level Threshold;

d is the maximum Service Credit (%) payable if the Achieved Service Level Reaches the Service Failure Threshold;

*m*is a coefficient defined for the services, which is calculated from the Formula *m = (d-c)/(a-b),* that is the slope of the straight line;

7.7 Consequently, the Service Credit regime is shown diagrammatically as follows:



7.8

7.9

7.10 The Service Credit (£) is subsequently derived as follows:

Service Credit (£) = contract charges x Service Credit (%)

7.11 An example Service Credit calculation for the Availability of a service, (offered herein for illustrative purposes only), is as follows:

Criteria	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
Availability	5.0	99.5%	95.00%	2.5%	25%

7.11.1 The Achieved Availability of a service was recorded as 97% for a Service Period. For this service, the Service Level Threshold is 99.5% and the Service Failure Threshold is 95%. The contract charges for the service for the Service Period are £3,000. Previous performance had exceeded the Service Level Threshold for Availability.

7.11.2 In this illustration example:

Service Credit % = 5.0 x (99.5-97.0) + 2.5 = 15%;

therefore the Service Credit calculation is:

Service Credit (£) = £3,000 x 15% = £450.

7.12 An example Service Credit calculation for Incident Resolution is as follows:

Criteria	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
Incident Resolution	0.25	95.0%	85.00%	2.5%	5%

7.12.1 The Service Level Threshold is 95% of all incidents to be resolved within a specified time with the Service Failure Threshold being 85%. Assume that the Buyer has 80 Incidents within a Service Period, 10 of which were not resolved within the specified time. Therefore, the Achieved Incident Resolution is 87.5% for the Service Period. The contract charges for all the services that the Buyer is consuming are £50,000 per Service Period. Previous performance had exceeded the Service Level Threshold for Incident Resolution Times.

7.12.2 In this illustration example:

Service Credit % = 0.25 x (95-87.5) + 2.5 = 4.375%

Consequently, the illustrated Service Credit calculation is:

Service Credit (£) = £50,000 x 4.375% = £2,187.50.

PART B Annex 1: Long Form Services Levels and Service Credits Table

8. Availability

8.1 **Services** (excluding the Service Desk)

Service Maintenance Level	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
1	N/A	N/A	N/A	N/A	N/A
2	1.3	95%	80%	5%	25%
3	2.86	97%	90%	5%	25%
4	5	99%	95%	5%	25%

8.2 **Service Desk**

Service Maintenance Level	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
All	5	99%	95%	5%	25%

9. Incident Resolution

Number of Incidents per Service Period	Coefficient (m)	Service Level Threshold (a)	Service Failure Threshold (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
39 or fewer	Not applicable	No more than 2 Incidents are Resolved in excess of the max Incident Resolution Times	5 or more Incidents are Resolved in excess of the max Incident Resolution Times	2.5% (payable when 3 Incidents breach the Service Level Threshold in any Service Period)	5% (payable when 4+ Incidents breach the Service Level Threshold in any Service Period)
40 and more	0.25	95%	85%	2.5%	5%

10. Quality

10.1 Service Desk:

Criteria	Coefficient	Service Level Threshold	Service Failure Threshold	Minimum Service Credit	Maximum Service Credit
Calls Answered within 60 seconds	0.25	90%	80%	2.5%	5%
Email Responded to within one (1) Working Day	0.083	90%	60%	2.5%	5%
Abandoned Calls	0.25	95%	85%	2.5%	5%

10.2 Data Service

10.2.1 Where the Buyer has procured Services that include data services, the following provisions will apply:

(a) The Services will only be deemed to have been Delivered once the Buyer has tested and accepted the quality of the data service;

(b) Subsequent to Services commencement, where the Buyer believes the quality of the data service is not acceptable:

(i) an Incident will be raised with the Service Desk;

(ii) the Supplier shall investigate the Incident;

(iii) Subsequent to the investigation, if:

(A) a fault is found, the Incident is Resolved as any other Incident;

(B) a fault is not found and the Buyer still believes the quality of the data service is unacceptable, the Supplier shall evidence to the Buyer that the data service complies with relevant Standards.

(iv) In the event that a fault is not found and the Supplier cannot evidence to the satisfaction of the Buyer that the data service complies with relevant Standards, the Service will be deemed Unavailable from the time that the Incident was first raised with the Service Desk and the Incident Resolution Time will be accordingly measured from that time.

10.3 Voice Service

10.3.1 Where the Buyer has procured Services that include voice services, the following provisions will apply:

(a) The Services will only be deemed to have been Delivered once the Buyer has tested and accepted the quality of the voice service;

(b) Subsequent to Services commencement, where the Buyer believes the quality of the voice service is not acceptable:

(i) an Incident will be raised with the Service Desk;

(ii) the Supplier shall investigate the Incident;

(iii) Subsequent to the investigation, if:

(A) a fault is found, the Incident is Resolved as any other Incident;

(B) a fault is not found and the Buyer still believes the quality of the voice service is unacceptable, the Supplier shall evidence to the Buyer that the voice service complies with relevant Standards.

(iv) In the event that a fault is not found and the Supplier cannot evidence to the satisfaction of the Buyer that the voice service complies with relevant Standards, the Service will be deemed Unavailable from the time that the Incident was first raised with the Service Desk and the Incident Resolution Time will be accordingly measured from that time.

PART B Annex 2: Critical Service Level Failure

1. CRITICAL SERVICE LEVEL FAILURE

1.1 A Critical Service Level Failure will be deemed to have occurred if the performance of the Services falls below the same Service Failure Threshold on three (3) occasions in any six (6) consecutive Service Periods.

1.2 In the event of a Critical Service Level Failure, the Buyer shall be entitled to terminate this Call-Off Contract for material Default.

PART C: Performance Monitoring

1. Performance Monitoring and Performance Review

1.1 Part C to this Call-Off Schedule provides the methodology for monitoring the provision of the Services:

1.1.1 to ensure that the Supplier is complying with the Service Levels; and

1.1.2 for identifying any failures to achieve Service Levels in the performance of the Supplier and/or provision of the Services (may also be referred to as a "Performance Monitoring System").

1.2 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.

1.3 The Supplier shall report all failures to achieve Service Levels and any Critical Service Level Failure to the Buyer in accordance with the processes agreed in Paragraph 1.2 of Part C of this Call-Off Schedule above.

1.4 The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") in accordance with the process and timescales agreed pursuant to paragraph 1.2 of Part C of this Call-Off Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

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

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

1.4.3 details of any Critical Service Level Failures;

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

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

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

1.5 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 (unless otherwise agreed):

1.5.1 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;

1.5.2 be attended by the Supplier's representative and the Buyer's representative; and

1.5.3 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.

1.6 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.

1.7 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.

2. Satisfaction Surveys

2.1 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.

PART C ANNEX 1: ADDITIONAL PERFORMANCE MONITORING REQUIREMENTS

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

1. Definitions

1.1 In this Schedule, which shall apply only where so specified by a Buyer that has undertaken a Further Competition, 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 2.1 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 Annex A of this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager shall be:

4. 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;

5. 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;

6. able to cancel any delegation and recommence the position himself; and

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

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

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

8. Contract Risk Management

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

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

8.2.1 the identification and management of risks;

8.2.2 the identification and management of issues; and

8.2.3 monitoring and controlling project plans.

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

8.4 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.

9. Role of the Operational Board

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

10. GOVERNANCE STRUCTURE

11. The Parties shall establish the Governance Structure described in the diagram below and Appendix 1, which comprises the following Boards:
    12. Supplier Governance Board;
    13. Commercial and Services Board;
    14. Exit and Transition Board;
    15. Service Implementation Board (which shall only operate during the implementation of Transition).
    16. Supplier Performance Review Board (acting as a feeder to the Commercial & Services Board);
    17. Commercial Review Meetings (acting as a feeder to the Commercial & Services Board); and

18. BOARD STRUCTURE & REPRESENTATION

19. This Schedule describes in relation to each Board:
    20. the Customer Authority's Board Members;
    21. the Contractor's Board Members;
    22. the responsibilities and functions of each Board;
    23. the frequency at which each Board shall meet (unless agreed otherwise) including the date, time and location of the first and subsequent meetings.
24. The Governance Structure comprises cross-functional and cross-organisational representation with the intent that these Representatives shall work co-operatively to enable successful execution of this Agreement.
25. In addition to the Boards described in appendices, any one or more Sub-Group(s) may be established.
26. The Customer Authority and the Contractor shall, in addition to the Boards identified in Paragraph 6.1, appoint suitably senior and experienced individuals to conduct the activities identified.

27. Replacement of Personnel

28. Without prejudice to Call Off Schedule 7 (Key Supplier Staff), if either Party wishes to replace any Board Member position, that Party shall notify the other in writing of the proposed change for agreement by the other Party (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing, it is intended that each Customer Authority's Board Member has at all times a counterpart Contractor's Board Member of equivalent seniority and expertise.

29. BOARD MEETINGS

30. Attendees

Each Party shall ensure that:

31. its Board Members attend each Board meeting at which that Board Member's attendance is required, or

32. if any Board Member is not able to attend a Board meeting, that Board Member shall use all reasonable endeavours to ensure that:

(a) a delegate attends the relevant Board meeting in place, who has the same authority in relation to that Board as the Board Member and (wherever possible) is properly briefed and prepared; and

(b) he/she is debriefed by such delegate after the relevant Board meeting.

33. Attendance at the Board meetings shall be in person or, where agreed in advance by both Parties, by video conference or voice teleconference.

34. The Parties may, by mutual agreement and having regard to the items for discussion at that Board meeting, invite other attendees to any Board meeting where such attendees shall be Customer Authority or Contractor employees or employees of any Sub-contractor or third party suppliers and these attendees shall be subject to obligations of confidentiality.

35. Chairperson

8.2.1 The Customer Authority shall appoint a chairperson for each Board. The chairperson (or their nominated representative) shall be responsible for:

36. scheduling Board meetings according to an agreed rolling calendar of dates;

37. setting the agenda for the Board meetings and circulating to all attendees in advance of such meeting;

38. ensuring that all necessary papers and reference documents relevant to each agenda item are circulated in accordance with the meeting frequency set out in the relevant Meeting Charter;

39. ensuring that appropriate notices and (if necessary) reminder notices are properly prepared and distributed to all attendees sufficiently in advance of the Board meetings;

40. where the attendance of any Board Member is described in a Meeting Charter as being on an "as appropriate" basis, maintaining liaison with the Parties to determine which of those attendees is required to attend each Board meeting and ensure that such attendees are notified of the requirement for their attendance accordingly;

41. chairing the Board meetings;

42. monitoring the progress of any follow-up tasks and activities agreed to be carried out following the Board meetings;

43. ensuring that minutes for the Board meetings are recorded, agreed and disseminated electronically to the appropriate persons and to all the Board meeting participants promptly within seven (7) calendar days after the Board meeting. The Parties acknowledge that such minutes do not replace individual Board Members' responsibility to record and progress actions;

44. facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner and ensuring that appropriate individuals are notified accordingly; and

45. General

8.3.1 Board meetings shall be quorate as long as at least two (2) representatives from each Party are present. Each Board meeting shall be convened at the relevant frequency specified in the relevant Meeting Charter.

8.3.2 The Parties shall ensure, as far as reasonably practicable, that all the Boards shall as soon as practicably possible resolve the issues and achieve the objectives placed before them. Each Party shall use all reasonable endeavours to ensure that the Board Members are empowered to make relevant decisions or have any necessary access to empowered individuals for decisions to be made to achieve this.

8.3.3 Where either Party becomes aware of an urgent or important issue which it has been unable to resolve without calling a meeting of the relevant Board it may request an urgent meeting of that Board. Such requests shall be made to the Chairperson of the relevant Board who shall not unreasonably refuse such request and, if such request is granted, shall co-operate with the requesting Party to arrange for a meeting of the relevant Board to be convened as soon as reasonably practicable.

8.3.4 Any issue that cannot be resolved between the Parties within a Board shall be escalated to the next level for resolution up to the Supplier Governance Board.

46. SUPPLIER PERFORMANCE REVIEWS

Supplier Performance Review Board meetings shall be held on a monthly basis no later than one (1) week following the provision of the Performance Monitoring Reports. The Supplier Performance Scorecard shall be the focal point of discussion and relevant supporting material shall be presented as required. The meeting shall be chaired by the Customer Authority. Agendas shall be distributed three (3) working days before the meeting. A formal note of the meeting and the approved Supplier Performance Scorecard shall be issued to

the authorised recipients within three (3) working days of the Supplier Performance Review Board having been held, by the Customer Authority.

47. Key Performance Reporting

48. As part of the government's transparency agenda (https://www.gov.uk/government/publications/key-performance-indicators-kpis-for-governments-most-important-contracts) , information on performance against Key Performance Indicators (KPIs) and/or Service Level Agreements (SLAs) will be shared with Cabinet Office and published on gov.uk on a quarterly basis.

49. The Supplier is obliged to provide performance information monthly as part of the Supplier Performance Review, using the format described in Annex B of this Schedule.

50. The Buyer will select the top 3 Key Performance Indicators or Service Level Agreements, as described in Schedule 14 of the Mobile Voice and Data Services agreement to be measured.

51. The following thresholds will apply:

- **Good** - Contractual target
- **Approaching Target** - Performance just below contractual target but not a major cause for concern unless underperformance is sustained
- **Requires Improvement** - Interventions required
- **Inadequate** - Major interventions or contractual rectification plans required. The Inadequate threshold must be any performance that is worse than Requires Improvement. For example, if the Requires Improvement threshold is “95%”, Inadequate must be defined as “Less than 95%”.

Annex A: Contract Boards

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

BOARD STRUCTURES AND FUNCTIONS

Supplier Governance Board	
Customer Authority members	TBC
Contractor members	TBC
Responsibilities and Functions	[redacted]
Frequency	Quarterly.

Commercial & Services Board
TBC
TBC
[redacted]

Service Implementation Board	
Customer Authority members	TBC
Contractor members	TBC
Responsibilities and Functions	[redacted]

Frequency	Weekly (unless otherwise agreed by its members) during implementation.

Exit and Transition Board	
Customer Authority members	TBC
Contractor members	TBC
Responsibilities and Functions	[redacted]
Frequency	No less than once per Contract Year, and as required in order to effectively manage updates and implementation of the Exit Plan.

Supplier Performance Review Board	
Customer Authority members	TBC
Contractor members	TBC
Responsibilities and Functions	a) [redacted]
Frequency	Monthly or as required by the Customer Authority from time to time. To be held before the monthly Services Board.

Annex B: PERFORMANCE REPORTING

	Good Target	Approaching Target Threshold	Requires Improvement Threshold	Inadequate Threshold
KPI 1 (Name/Description TBC)	%	%	%	%
KPI 2 (Name/Description TBC)	%	%	%	%
KPI 3 (Name/Description TBC)	%	%	%	%

RM3808 Call-Off Schedule 16 (Benchmarking)

1. Definitions

1.1. In this Schedule, the following expressions shall have the following meanings:

"Benchmarked Rates"	the Charges for the Benchmarked Deliverables;
"Benchmarker"	a neutral and independent third party with knowledge and experience of financial matters in relation to the Benchmarked Deliverables;
"Benchmark Review"	a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value;
"Benchmarked Deliverables"	any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule;
"Comparable Rates"	rates payable by the Comparison Group for Comparable Deliverables that can be fairly compared with the Charges;
"Comparable Deliverables"	deliverables that are identical or materially similar to the Benchmarked Deliverables (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar Deliverables exist in the market, the Supplier shall propose an approach for developing a comparable Deliverables benchmark;
"Comparison Group"	a sample group of organisations providing Comparable Deliverables which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be fair comparators with the Supplier or which, are best practice organisations;
"Equivalent Data"	data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group;
"Good Value"	that the Benchmarked Rates are within the Upper Quartile; and
"Upper Quartile"	in respect of Benchmarked Rates, that based on an analysis of Equivalent Data, the Benchmarked Rates, as compared to the range of prices for Comparable Deliverables, are within the top 25%

in terms of best value for money for the recipients of Comparable Deliverables.

2. When you should use this Schedule

2.1. This Schedule shall apply where so specified by a Buyer that has undertaken a Further Competition.

2.2. The Supplier acknowledges that the Buyer wishes to ensure that the Deliverables, represent value for money to the taxpayer throughout the Contract Period.

2.3. This Schedule sets to ensure the Contracts represent value for money throughout and that the Buyer may terminate the Contract by issuing a Termination Notice to the Supplier if the Supplier refuses or fails to comply with its obligations as set out in Paragraphs 3 of this Schedule.

2.4. Amounts payable under this Schedule shall not fall with the definition of a Cost.

3. Benchmarking

3.1. How benchmarking works

3.1.1. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

3.1.2. The Buyer may, by written notice to the Supplier, require a Benchmark Review of any or all of the Deliverables.

3.1.3. The Buyer shall not be entitled to request a Benchmark Review during the initial 24 Month period from the Contract Commencement Date or at intervals of less than twelve (12) Months after any previous Benchmark Review.

3.1.4. The purpose of a Benchmark Review will be to establish whether the Benchmarked Deliverables are, individually and/or as a whole, Good Value.

3.1.5. The Deliverables that are to be the Benchmarked Deliverables will be identified by the Buyer in writing.

3.1.6. Upon its request for a Benchmark Review the Buyer shall nominate a Benchmarker. The Supplier must approve the nomination within ten (10) Working Days unless the Supplier provides a reasonable explanation for rejecting the appointment. If the appointment is rejected then the Buyer may propose an alternative Benchmarker. If the Parties cannot agree the appointment within twenty (20) days of the initial request for Benchmark review then a Benchmarker shall be selected by the Chartered Institute of Financial Accountants.

3.1.7. The cost of a Benchmarker shall be borne by the Buyer (provided that each Party shall bear its own internal costs of the Benchmark Review) except where the Benchmark Review demonstrates that the Benchmarked Service and/or the Benchmarked Deliverables are not Good Value, in which case the Parties shall share the cost of the Benchmarker in such proportions as the Parties agree (acting reasonably). Invoices by the Benchmarker shall be raised against the Supplier and the relevant portion shall be reimbursed by the Buyer.

3.2. Benchmarking Process

3.2.1. The Benchmarker shall produce and send to the Buyer, for Approval, a draft plan for the Benchmark Review which must include:

a) a proposed cost and timetable for the Benchmark Review;

b) a description of the benchmarking methodology to be used which must demonstrate that the methodology to be used is capable of fulfilling the benchmarking purpose; and

c) a description of how the Benchmarker will scope and identify the Comparison Group.

3.2.2. The Benchmarker, acting reasonably, shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking.

3.2.3. The Buyer must give notice in writing to the Supplier within ten (10) Working Days after receiving the draft plan, advising the Benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the Benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan.

3.2.4. Once both Parties have approved the draft plan then they will notify the Benchmarker. No Party may unreasonably withhold or delay its Approval of the draft plan.

3.2.5. Once it has received the Approval of the draft plan, the Benchmarker shall:

a) finalise the Comparison Group and collect data relating to Comparable Rates. The selection of the Comparable Rates (both in terms of number and identity) shall be a matter for the Benchmarker's professional judgment using:

i. market intelligence;

ii. the Benchmarker's own data and experience;

iii. relevant published information; and

iv. pursuant to Paragraph In carrying out the benchmarking analysis the Benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data: below, information from other suppliers or purchasers on Comparable Rates;

b) by applying the adjustment factors listed in Paragraph In carrying out the benchmarking analysis the Benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data: and from an analysis of the Comparable Rates, derive the Equivalent Data;

c) using the Equivalent Data, calculate the Upper Quartile;

d) determine whether or not each Benchmarked Rate is, and/or the Benchmarked Rates as a whole are, Good Value.

3.2.6. The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the Benchmarker in order to undertake the benchmarking. The Supplier agrees to use its reasonable endeavours to obtain information from other suppliers or purchasers on Comparable Rates.

3.2.7. In carrying out the benchmarking analysis the Benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data:

a) the contractual terms and business environment under which the Comparable Rates are being provided (including the scale and geographical spread of the customers);

b) exchange rates;

c) any other factors reasonably identified by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive.

3.3. Benchmarking Report

3.3.1. For the purposes of this Schedule "Benchmarking Report" shall mean the report produced by the Benchmarker following the Benchmark Review and as further described in this Schedule;

3.3.2. The Benchmarker shall prepare a Benchmarking Report and deliver it to the Buyer, at the time specified in the plan Approved pursuant to Paragraph The Buyer must give notice in writing to the Supplier within ten (10) Working Days after receiving the draft plan, advising the Benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the Benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan., setting out its findings. Those findings shall be required to:

a) include a finding as to whether or not a Benchmarked Service and/or whether the Benchmarked Deliverables as a whole are, Good Value;

b) if any of the Benchmarked Deliverables are, individually or as a whole, not Good Value, specify the changes that would be required to make that Benchmarked Service or the Benchmarked Deliverables as a whole Good Value; and

c) include sufficient detail and transparency so that the Buyer can interpret and understand how the Benchmarker has calculated whether or not the Benchmarked Deliverables are, individually or as a whole, Good Value.

3.3.3. The Parties agree that any changes required to this Contract identified in the Benchmarking Report shall be implemented at the direction of the Buyer in accordance with Clause 24 (Changing the contract).

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 Buyer under this Call-Off Contract.

BUYERS REQUIREMENTS

The Department for Education (the "Buyer"), has a requirement for a mobile voice and data telephony service. The buyer wishes to procure SIMs for the buyer's estate with data and voice connectivity, which enables staff to work flexibly and 'on-the-go' and continue to deliver departmental priorities.

The requirements detailed below list the minimum specification. Following contract award the Buyer and Supplier will jointly agree the final services to be delivered to take account of the Suppliers proposed delivery model.

Minimum Requirements

- All-Inclusive Call Tariff
- Data Services (Data as a Shared Data Bundle and Data connections on a per connection basis).
- Service Management Services
- The Department requires Wi-Fi-Calling functionality on devices.

Optional Requirements

1.6.2 The Department may also require the provision of additional services throughout the contract term, including:

- Transferable Data Management Software Licences for use on selected devices.

1.7 The Supplier shall not apply a cap or usage limit to the services detailed within section 2 and 3 below. Any excessive usage will be notified to the Buyer through exception reporting.

1.8 Unless agreed otherwise with the Buyer, the Supplier shall automatically bar International data, voice calls and SMS.

1.9 The Supplier shall provide the ability to bar access to defined call types for all End Users, groups of End Users or individual End Users at no additional charge including but not limited to:

- Premium Rate numbers;
- International dial unless approved by the Buyer;
- MMS / Photo Messaging.
- Wi-fi calling

1.10 The Supplier shall add or remove service bars upon request by the Buyer. The Supplier shall be liable for all usage charges for these services where it is found that:

- a bar was not in place when one was requested by the Buyer and the Buyer can evidence that request was logged by the Supplier; and
- when a bar was requested by the Buyer and acknowledged as in place by the Supplier.

1

1.11 The Supplier shall not prohibit emergency calls regardless of whether any bar has been put in place.

The Supplier shall provide all SIM cards free of charge, including replacement SIMS where the original SIM card is no longer the correct size for the end user's new device, has been lost, stolen or subject to non-malicious damage

ALL INCLUSIVE TARIFF

1.1 The Department requires an All-inclusive Call Tariff including:

- SIM only with SIM tray opening tool
- Tariff to include line rental set at £0.00 (Zero);
- No early termination fee per connection will apply.

Voice and SMS service to include the following types:

- UK Landline.
- UK Mobile Network.
- UK Non-geographic numbers prefixed: 0300, 0800, 0808, 0500, 116 & local rate, free phone numbers.
- Mobile SMS.
- Voicemail / Answerphone.
- EU voice and SMS roaming.
- Cap free all-inclusive tariff with excessive usage being notified via exception reporting.
- Ability to add usage caps to connections.
- Barred international voice calls and SMS unless agreed and enabled.
- Ability to bar access to defined call types for all End Users, groups of End Users or individual End Users at no additional charge including but not limited to:

2 • Premium Rate numbers.
3 • International dial unless approved by the Customer.
4 • MMS / Photo Messaging.

- Allow emergency calls regardless of any bar in place.

DATA SERVICES

4.1 The Department requires a Shared 4G Data Bundle for UK and EU roaming data.

4.2 The Department requires a range of data services in various increments, and if possible, an unlimited shared data bundle. Shared data bundles can be flexed up or down without restriction or early termination fee.

4.3 The Department requires a flexible approach to number of connections accessing different data services, with cost of shared data bundle being irrespective of number of connections. The Department require the ability to add and remove connections within the bundle with no minimum or maximum constraints on volumes.

4.4 The Department requires a 4G data only package (500MB up to Unlimited) on a per connection basis for UK and EU roaming data.

4.5 Out of bundle over usage charges to be clearly defined.

4.6 All data services usable in conjunction with any data enabled mobility device that will take a SIM card and allow tethering at no extra charge.

4.7 The Department would like the ability to assign individual data caps.

The charge for the Data services will be a fixed monthly recurring charge.

The Department would be interested in considering 5G and eSIM options in the future. Suppliers are invited to supply their future road map with their submission.

TRANSITION SUPPORT SERVICE

4.1 The Supplier shall support the Buyer in implementing the new service. Support should be provided for the following activities, although not limited to:

- Set-up and installation of SIMs;
- Troubleshooting connectivity issues;
- Porting issues;
- Unlocking handsets.

4.2 The Customer must be able to access transition support services through a dedicated telephone number available as a minimum between 9am and 5pm Monday to Friday, excluding Bank Holidays, throughout the Term. The Customer must also be assigned a dedicated suitable Transition Manager who will lead the transition as part of the onboarding.

4.3 Transition support will cover all sites within the Customer estate identified in the Implementation Plan. There will be no minimum number of connections per Customer site for the purpose of transition support.

4.4 The Contractor must complete the tariff build within 5 days from Contract Award.

4.5 Any connections identified as available by the Customer for transition that are not migrated within 3 months from notification to the Contractor will be subject to a Delay Payment charge

SERVICE MANAGEMENT

4.1 The Department requires service management to support the management of their mobile estate.

4.2 Ability to access the account management service through a dedicated telephone number available 9am to 5pm Monday to Friday excluding Bank Holidays as a minimum throughout the Call Off Contract Period.

4.3 Facilities not provided via an online portal must be accessible via the account management services with clearly communicated response timescales.

4.4 The Department requires access to an online portal, which enables the Department to:

- Place Orders (eOrdering);
- Undertake moves, adds and changes to data bundles.
- Check Order Status;
- Make payments electronically (ePayment);
- Access online account management services;
- Ask customer support and technical support questions;
- Receive alerts for each connection, account or cost code;
- Run compile and receive reports including real-time data;
- Add additional log-on details for additional users, upon request;
- Tier access rights to accommodate different types of users, such as Administrator, Account/Cost Code Manager, Team Manager;
- Assign user names, email address and relevant Customer identifiers to the phone numbers for reporting purposes.
- Tiered accounts to generate separate invoices and locked access to each account for individuals.
- End user information on usage and cost if available.

In the event a supplier does not offer an online portal, an alternative solution must be provided to manage this requirement.

5.4 The Department requires access to comprehensive reports and reporting tools to allow the Department to understand their use of Services. The Department requires this as close to real-time data as possible.