ORDER FORM

CALL-OFF REFERENCE:	**Project**_ 4781
THE BUYER:	**THE SECRETARY OF STATE FOR EDUCATION**
BUYER ADDRESS	Sanctuary Buildings, 20 Great Smith Street, London, SW1P 3BT
THE SUPPLIER:	**COMPUTACENTER (UK) LIMITED**
SUPPLIER ADDRESS:	Hatfield Ave, Hatfield, AL10 9TW
REGISTRATION NUMBER:	01584718
DUNS NUMBER:	22-602-3463
SID4GOV ID:	Not applicable

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 01 September 2020.

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

CALL-OFF LOT(S):

Lot 3 Software & Associated Services

CALL-OFF INCORPORATED TERMS

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

(A) This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.

(B) Joint Schedule 1(Definitions and Interpretation) RM6068

(C) The following Schedules in equal order of precedence:

- Joint Schedules for RM6068

  Joint Schedule 2 (Variation Form)

  Joint Schedule 3 (Insurance Requirements)

  Joint Schedule 4 (Commercially Sensitive Information)

  Joint Schedule 10 (Rectification Plan)

  Joint Schedule 11 (Processing Data)

- Call-Off Schedules for Project_ 4781

  Call-Off Schedule 1 (Transparency Reports)

  Call-Off Schedule 5 (Pricing Details)

  Call-Off Schedule 6 (ICT Services)

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

Call-Off Schedule 9 (Security)

Call-Off Schedule 10 (Exit Management)

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

Call-Off Schedule 20 (Call-Off Specification)

(D) CCS Core Terms (version 3.0.6)

(E) Annexes A to E Call-Off Schedule 6 (ICT Services)

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

CALL-OFF SPECIAL TERMS

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

Special Term 1: **REDACTED**

Special Term 2: **REDACTED**

Special Term 3: **REDACTED**

Special Term 4: **REDACTED**.

Special Term 5:

Modern Slavery, Child Labour and Inhumane Treatment

5.1 The Supplier:

5.1.1 shall not use, or 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 identity papers with the Employer or deny Supplier staff freedom to leave their employer after reasonable notice;

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

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

5.1.6 shall have and maintain throughout the Term of the Call-Off Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and shall 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 this Call-Off Contract;

5.1.8 shall prepare and deliver to the Buyer within fourteen (14) days of the Start Date and updated on a frequency defined by the Department, a 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;

5.1.9 shall not use, or 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 its Subcontractors to use, child or slave labour;

5.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to the Buyer and Modern Slavery Helpline1.

Special Term 6: **REDACTED**

CALL-OFF START DATE:	01 September 2020
CALL-OFF EXPIRY DATE:	30th September 2021
CALL-OFF INITIAL PERIOD:	13 Months
CALL-OFF OPTIONAL EXTENSION PERIOD	12 Months

CALL-OFF DELIVERABLES

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

LOCATION FOR DELIVERY

Title to Goods is transferred to the Buyer on payment to the Supplier in full (save in respect of software where title to the same shall remain at all times with the relevant licensor).

DATES FOR DELIVERY OF THE DELIVERABLES

The Licences will be made available for use by the Buyer in the Cisco Umbrella portal after receipt and processing of the Supplier's order by Cisco.

TESTING OF DELIVERABLES

Not applicable

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be the duration of any guarantee or warranty period the Supplier has received from the third party manufacturer or supplier.

[1] The "Modern Slavery Helpline" refers to the point of contact 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.

MAXIMUM LIABILITY

REDACTED CALL-OFF CHARGES

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

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

The Supplier shall submit invoices directly to the billing address 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:

Department for Education
Sanctuary Buildings
20 Great Smith Street
London
SW1P 3BT

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED REDACTED REDACTED BUYER'S ENVIRONMENTAL POLICY

Not applicable

BUYER'S SECURITY POLICY

See Call-Off Schedule 9

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED REDACTED REDACTED REDACTED

SUPPLIER'S CONTRACT MANAGER

REDACTED REDACTED REDACTED REDACTED PROGRESS REPORT FREQUENCY

See Call-Off Schedule 1 (Transparency Reports)

PROGRESS MEETING FREQUENCY

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

KEY STAFF

Not applicable

KEY SUBCONTRACTOR(S)

Not Applicable

COMMERCIALLY SENSITIVE INFORMATION

The details of the Supplier's Commercially Sensitive Information are contained in Joint Schedule 4 (Commercially Sensitive Information)

SERVICE CREDITS

Not Applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

Not applicable

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

Joint Schedule 4

Commercially Sensitive Information

1. WHAT IS THE COMMERCIALLY SENSITIVE INFORMATION?

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

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

No.	Date	Item(s)	Duration of Confidentiality
	14th May 2020	Special Terms	Term + 2 Years
		Buyer's Authorised Representative	
		Suppliers Authorised Representative	
		Suppliers Contract Manager	
		Joint Schedule 3 (Insurance Requirements)	
		Paragraphs 1.1.1, 1.3, 1.4 and 4 of Call-Off Schedule 5 (Pricing Details)	
		Schedule 8 (BCDR)	

Joint Schedule 11

Processing Data

Status of the Controller

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

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

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

1.3 "Joint Controller" with the other Party;

1.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

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

Where one Party is Controller and the other Party its Processor

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

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

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

4.1 a systematic description of the envisaged Processing and the purpose of the Processing;

4.2 an assessment of the necessity and proportionality of the Processing in relation to the Services;

4.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

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

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

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

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

5.2.1 nature of the data to be protected;

5.2.2 harm that might result from a Data Loss Event;

5.2.3 state of technological development; and

5.2.4 cost of implementing any measures;

5.3 ensure that:

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

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

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

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

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

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

5.4 not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

5.4.1 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;

5.4.2 the Data Subject has enforceable rights and effective legal remedies;

5.4.3 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

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

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

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

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

6.2 receives a request to rectify, block or erase any Personal Data;

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

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

6.5 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

6.6 becomes aware of a Data Loss Event.

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

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

8.1 the Controller with full details and copies of the complaint, communication or request;

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

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

8.4 assistance as requested by the Controller following any Data Loss Event; and/or

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

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

9.1 the Controller determines that the Processing is not occasional;

9.2 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

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

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

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

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

12.1 notify the Controller in writing of the intended Subprocessor and Processing;

12.2 obtain the written consent of the Controller;

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

12.4 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

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

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

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

ANNEX 1

Processing Personal Data

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

1. The contact details of the Relevant Authority's Data Protection Officer are:

1.1 Name: **REDACTED**

1.2 Email: **REDACTED**

1.3 Address: **REDACTED**

1.4 Telephone: **REDACTED**

2. The contact details of the Supplier's Data Protection Officer are: **REDACTED**.

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

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

5. For information only, the Master Data Protection Agreement between the Relevant Authority and Cisco is attached at Schedule 6 (ICT Services).

Personal Data Processing Description

Description	Details
Identity of Controller for each Category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the Personal Data that the Supplier Processes on behalf of the Relevant Authority and in accordance with its instructions in the performance of the Services.
Duration of the Processing	For the duration of the provision of the Services and as otherwise permitted in the Contract.
Nature and purposes of the Processing	The Personal Data will be Processed for the purposes of performing the Services and as otherwise permitted in the Contract. The nature of the Processing for these purposes could include any operation performed on Personal Data, 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).

	The Personal Data will be Processed for the purpose of performing the Services and as otherwise permitted in the Contract. The purposes include the ordering, and delivery of the Cisco licences.
Type of Personal Data	Personal Data that the Supplier Processes on behalf of the Relevant Authority and in accordance with its instructions in the performance of the Services.
Categories of Data Subject	Data Subjects of the Personal Data referred to above, which may include: (a) Staff (including volunteers, agents, and temporary workers) of the Relevant Authority. (b) Staff (including volunteers, agents, and temporary workers) of Responsible Bodies.
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**	As set out in paragraph 5.5 of this Joint Schedule 11.

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

It is key to the Buyer that regular reporting as set out below is adhered to. The principles that the Buyer and the Supplier have agreed in relation to the key data required to demonstrate the performance of the Supplier is based on the following principles:

1. The Supplier will procure that the Buyer will have access to the following reports as made available by the Cisco portal in accordance with the Cisco Umbrella: Reporting You Can Count On document annexed to this Call-Off Schedule 1 under Annex B. Should the Buyer require assistance with configuration of this portal, this will be provided by the Supplier and deducted from the innovation fund as set out in paragraph 1.1.1. of Call-Off Schedule 5.

Title	Content	Format	Frequency	Buyer Contact
Technical – Daily Dashboard Reporting	The Buyer will be able to access the below listed Dashboard reports (updated daily): **Security Overview—**Gives you a snapshot of your environment's security activities. **Security Activity—**Security-related activity in your environment, including malware, phishing, and all other security categories over the selected time period. Filterable by anonymous or aggregated data only, source IP, and security category. **Activity Search—**Activity from the identities in your environment over a selected time period. Filterable by anonymous or aggregated data only, source IP, response, content category, and security category. **Total Requests—**Total requests for destinations from your organization over the selected time period. Filterable by anonymous or aggregated data only. **Activity Volume—**Total queries within your organization broken down by security categories and results over the selected time period. Filterable by anonymous or aggregated data only. This report has two views: Snapshot (table) and Trend Over Time (graph).	Dashboard report	Updated Daily	**REDACTED**

	Categories: DNS requests that match a Content category (only records blocked domains). Destination Lists: DNS requests that match an item on the Block or Allow destination lists (e.g Global Block and Global Allow). Permitted: DNS requests that do not match a category or destination list but are allowed. **Top Identities—**A list of the top traffic-generating identities over the selected time period. Filterable by anonymous or aggregated data only. **Top Destinations—**A list of the most requested domains within your organization over the selected time period. Filterable by anonymous or aggregated data only, response, destination, content category, and security category. **Top Categories—**A list of the top content categories for your organization over the selected time period. Filterable by anonymous or aggregated data only and response. **Admin Audit Log—**A record of any configuration changes made to your settings by any of your Umbrella administrators.			

ANNEX B

Cisco Umbrella: Reporting You Can Count On

cisco-umbrella-repor
ting-you-can-count-o

Call-Off Schedule 5

Pricing Details

1. CHARGES

REDACTED

2. INVOICING

2.1 The Supplier will invoice the Buyer for the software licenses at the point when the licence key is issued by Cisco.

2.2 Invoices are payable on 30 days terms from receipt of the invoice.

3. ADDITIONAL INFORMATION

DESCRIPTION	INCLUDED IN CHARGES?
Travel and expenses	N/A
VAT	Excluded
Any duties or levies other than value added tax	Excluded

4. OPTIONAL SERVICES

REDACTED

4.1

Additional Services

Call-Off Schedule 6

ICT Services

1. DEFINITIONS

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

"Buyer Property"	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Defect"	any of the following: (a) any error, damage or defect in the manufacturing of a Deliverable; or (b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or (d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;
"Emergency Maintenance"	ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;

"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors (if any) 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 Sub-Contractor (if any) or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. WHEN THIS SCHEDULE SHOULD BE USED

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

3. BUYER DUE DILIGENCE REQUIREMENTS

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

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

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

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

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

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

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

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

3.2.3 a timetable for and the costs of those actions.

4. SOFTWARE WARRANTY

4.1 The Supplier represents and warrants that:

4.1.1 it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor (if any)) 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:

(a) be free from material design and programming errors;

(b) perform in all material respects in accordance with the relevant specifications and Documentation; and

(c) not infringe any IPR.

5. PROVISION OF ICT SERVICES

5.1 The Supplier shall:

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

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

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

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

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

6. STANDARDS AND QUALITY REQUIREMENTS

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

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

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

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

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

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

6.4.3 obey all lawful instructions and reasonable directions of the Buyer 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 Not Used

8.2 The Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

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

8.4 The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. INTELLECTUAL PROPERTY RIGHTS IN ICT

9.1 **Assignments granted by the Supplier: Specially Written Software**

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

(a) the Documentation, Source Code and the Object Code of the Specially Written Software; and

(b) 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:

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

(b) 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

(c) without prejudice to paragraph (b), 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:

(a) 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

(b) only use such third party IPR as referred to at paragraph 9.2.3 (a) if the Buyer Approves the terms of the licence from the relevant third party.

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

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

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

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

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

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

(a) will no longer be maintained or supported by the developer; or

(b) 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:

(a) a Central Government Body; or

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

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

9.5 **Licence granted by the Buyer**

9.5.1 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors (if any) provided that any relevant Sub-Contractor (if any) 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:

(a) suitable for publication by the Buyer as Open Source; and

(b) 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:

(a) 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;

(b) 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;

(c) do not contain any material which would bring the Buyer into disrepute;

(d) can be published as Open Source without breaching the rights of any third party;

(e) 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

(f) 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:

(a) 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

(b) 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:

(a) 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

(b) 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 Annex A of this Call-Off Schedule 6.

10.1.2 Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in Annex B of this Call-Off Schedule 6, together with the relevant third party provider's Master Data Protection Agreement which has been entered into with the Buyer and is attached for information purposes only.

10.2 Software Support & Maintenance Terms

10.2.1 Additional terms for provision of Software Support & Maintenance Services are detailed in Annex C of this Call-Off Schedule 6. The Supplier will procure that such Software Support & Maintenance Services provided to the Buyer by Cisco meet the service levels set out in the Service Level Agreement attached at Annex C of this Call-Off Schedule 6.

10.2.2 In addition to the Gold Support Service as detailed in the Software Support & Maintenance Service terms detailed in Annex C of this Call-Off Schedule 6, Cisco intends to make a Cisco Customer Success Manager (**CSM)** available to assist the Buyer and Buyer's authorised source as described below. Notwithstanding the foregoing, Cisco is not contractually obligated to provide such additional assistance and such assistance and CSM resources will only be provided by Cisco on an as-available basis. The additional assistance and resources set forth in paragraph 10.2.3 below are to be provided in Cisco’s sole discretion and subject to change without notice

10.2.3 .The CSM will assist the Buyer for the duration of the Contract. The CSM’s intended scope is limited to a post-sale account management/single point of contact role. The CSM may provide product utilization information, educational resources, address concerns, and act as an escalation path for the Buyer.

10.3 Software as a Service Terms

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

10.4 Device as a Service Terms

10.4.1 Additional terms for provision of a Device as a Service solution are detailed in Annex E to this Call-Off Schedule 6;

10.4.2 Where Annex E is used the following Clauses of the Core Terms shall not apply to the provision of the Device as a Service solution:

Clause 8.7

Clause 10.2

Clause 10.3.2]

11. CUSTOMER PREMISES – NOT USED

ANNEX A

Non-COTS Third Party Software Licensing Terms

The Supplier shall provide details of all Non-COTS Third Party Software Licensing Terms within ten (10) Working Days of contract signature. Third party software (if any) shall be licensed subject to the third party licensor's standard license terms which shall govern the supply, the Buyer's use of and obligations relating to the software in their entirety.

ANNEX B

COTS Licensing Terms

Third party software (if any) shall be licensed subject to the third party licensor's standard license terms attached which shall govern the supply, the Buyer's use of and obligations relating to the software in their entirety.

Cisco-Umbrella-Enterprise-Terms-of-Ser

Cisco Master Data Protection Agreement

clean7sep20Cisco Master Data Protectic

ANNEX C

Software Support & Maintenance Terms

Third party services (if any) shall be supplied subject to the applicable third party's standard service terms.

ODNS_Support_SLA_Gold3.pdf

Cisco Umbrella Service Level Agreement & Gold Support Service

1. General.

Cisco Umbrella will provide the Services according to the service guarantees in this Service Level Agreement ("SLA"). For the purposes of this SLA, "Services" shall be defined as our RFC Recursive DNS service and does not include web-based user interfaces, configuration systems or other data access or manipulation methods.

2. Service Availability Commitment.

The Cisco Umbrella Services shall meet the following service level criteria:

- Services Availability: 99.999% each calendar month. Services Availability will be calculated by dividing the total number of minutes of uptime in the Services during an applicable calendar month by the total number of actual minutes in such month minus minutes of outages in the Services occurring during the Scheduled Maintenance Period (as defined in Section 6) or attributable to elements outside of Cisco Umbrella' reasonable control, and then multiplying that amount by 100. For the purposes of this calculation, "uptime" means the number of minutes where there were no outages, excluding outages for Scheduled Maintenance Periods as set below or attributable to elements outside of Cisco Umbrella' reasonable control as set forth below in Section 5.

If a dispute arises about whether or not an outage occurred, Cisco Umbrella shall make a determination in good faith based on its system logs, monitoring reports and configuration records, and Cisco Umbrella' records shall control.

3. Outage Reporting Process.

Customer must inform Cisco Umbrella' Customer Support Department in writing or by email to umbrella-support@cisco.com when Customer first believes that there has been an outage.

4. Remedy.

If the Services Availability for a given calendar month falls below 99.999% ("Service Unavailability"), provided that Customer has made a written request to Cisco Umbrella within fourteen (14) days of the time it first notices an outage, Cisco Umbrella will provide Customer with a Service Credit that can be applied for the next renewal subscription period. Service Credits are not payable unless Customer's Cisco Umbrella account is in good standing. Cisco Umbrella will

ANNEX D

Software as a Service Terms

N/A

ANNEX E

Device as a Service Terms

N/A

Call-Off Schedule 8

Business Continuity and Disaster Recovery

REDACTED

Call-Off Schedule 9

Security

Commodity Service Security Requirements

1. The Supplier will ensure that any Supplier system that processes Orders placed by the Buyer and invoices issued to the Buyer which holds any Buyer Data will comply with:

1.1 the Departmental Security Requirements (Annex 1)

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

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

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

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

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

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

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

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

ANNEX 1

1. DEPARTMENTAL SECURITY REQUIREMENTS

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**	shall have the meanings given to those terms by the Data Protection Act 2018

Processing

Buyer's Data **Buyer'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 Supplier by or Buyer; or (ii) (which the Supplier 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 **Buyer**	means the Department for Education
Departmental Security Standards	means the Buyer's security policy or any standards, procedures, process or specification for security that the Supplier 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	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP).
OFFICIAL-SENSITIVE	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 (ie 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 HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Suppliers which include but are not constrained to the following clauses.

1.2 Where the Supplier will provide products or services or otherwise handle information at OFFICIAL for the Buyer, 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; that "Suppliers supplying products or services to HMG shall have achieved, and will be expected to retain 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.

1.3 Where clause 1.2 above has not been met, the Supplier 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 Buyer. 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).

1.4 The Supplier 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 Supplier has an existing Protective Marking Scheme then the Supplier 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).

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 Supplier's or Subcontractor'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 1.14.

1.6 The Supplier 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.

1.7 The Supplier 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).

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

1.8.1 physical security controls;

1.8.2 good industry standard policies and processes;

1.8.3 malware protection;

1.8.4 boundary access controls including firewalls;

1.8.5 maintenance and use of fully supported software packages in accordance with vendor recommendations;

1.8.6 software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;

1.8.7 user access controls, and;

1.8.8 the creation and retention of audit logs of system, application and security events.

1.9 The Supplier 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 Supplier 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 Buyer except where the department has given its prior written consent to an alternative arrangement.

1.11 The Supplier 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.

1.12 Whilst in the Supplier'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".

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 Buyer 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 1.15.

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 Supplier 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 Supplier or sub-Supplier shall protect the Buyer’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.

1.16 Access by the Supplier or Subcontractor staff to Departmental Data 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 Buyer. All Supplier or Subcontractor staff must complete this process before access to Departmental Data is permitted.

1.17 All Supplier or Subcontractor employees who handle Departmental Data shall have annual awareness training in protecting information.

1.18 The Supplier 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 Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

1.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data 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 Suppliers, or other Security Standards pertaining to the solution.

Incidents shall be reported to the Buyer 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 Supplier 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 Supplier with outcomes being notified to the Buyer.

1.20 The Supplier 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 Buyer and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

1.21 The Supplier or Subcontractors 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 Supplier or Subcontractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.

1.22 The Buyer reserves the right to audit the Supplier or Subcontractors 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 Supplier's, and any Subcontractors', compliance with the clauses contained in this Section.

1.23 The Supplier and Subcontractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the Buyer. This will include obtaining any necessary professional security resources required to support the Supplier's and Subcontractor'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.

1.24 Where the Supplier is delivering an ICT solution to the Buyer 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 Supplier will provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer's expectation is that the Supplier shall provide written evidence of:

1.24.1 Compliance with HMG Minimum Cyber Security Standard.

1.24.2 Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.

1.24.3 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.

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

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

Call-Off Schedule 10

Exit Management

1. A minimum of three (3) months prior to the Expiry Date, the Supplier will provide the Buyer with a dedicated resource to assist the Responsible Bodies in the renewal or termination of their existing licences. A peer will also be provided by Cisco to ensure alignment between the Supplier and the Buyer.

2. No Supplier communication will be sent to the Responsible Bodies without the prior written consent of the Buyer.

Call-Off Schedule 15

Call-Off Contract Management

1. DEFINITIONS

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

"Operational Board"	the board established in accordance with paragraph 4 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. PROJECT MANAGEMENT

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

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

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

2.4 The Supplier shall liaise with Cisco and request that Cisco allocate a suitable resource to assist the Buyer.

3. ROLE OF THE SUPPLIER CONTRACT MANAGER

3.1 The Supplier's Contract Manager shall be:

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

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

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

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

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

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

4. ROLE OF THE OPERATIONAL BOARD

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

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

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

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

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

5. NOT USED

ANNEX

Contract Boards

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

Operational Board

1. Frequency of the Operational Board to be agreed within ten (10) Working Days of the Start Date.

2. In compliance with Government's COVID-19 distancing rules, Operational Boards shall take place via a Virtual Meeting Platform. The preferred Virtual Meeting Platform will be the one proposed by the Buyer.

3. Operational Board must have representatives from the Buyer and the Supplier.

Call-Off Schedule 20

Specification

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

1. THE REQUIREMENT

The Buyer is looking to procure a service that provides a safe and secure route to the internet (regardless of ISP), for Microsoft Windows and Google Chrome book devices. It is expected that Windows based devices will be imaged with required configuration to be safe and secure 'out of the box'.

It is expected that the Supplier will assume all support and maintenance responsibilities for the initial configuration, onboarding and ongoing management of the service, but allow the Buyer administrative access to allow the Buyer review, monitoring and input into the processes.

Requirement / Deliverables:

E-safety

In line with DfE statutory guidance set out in the KCSIE guidance https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 internet content filtering must be in place to prevent children from accessing illegal and inappropriate internet content and to ensure children are safe from terrorist and extremist material.

Illegal Content

Devices must have measures in place to prevent access to illegal internet content, specifically;

- A content filtering system that subscribes to IWF (Internet Watch Foundation) block list of illegal Child Sexual Abuse Material (CSAM)
- Integrate 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' https://www.gov.uk/government/publications/prevent-duty-guidance

Inappropriate Online Content

Device filtering must prevent access to the following categories of inappropriate internet content:

- **Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010**
- **Drugs / Substance abuse:** displays or promotes the illegal use of drugs or substances
- **Extremism:** promotes terrorism and terrorist ideologies, violence or intolerance
- **Malware / Hacking:** promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, with the exception of content that is strictly educational
- **Pornography:** displays sexual acts or explicit images
- **Piracy and copyright theft:** includes illegal provision of copyrighted material
- **Self-Harm:** promotes or displays deliberate self-harm (including suicide and eating disorders)

- **Violence:** Displays or promotes the use of physical force intended to hurt or kill

This list should not be considered exhaustive and providers will be able to demonstrate how their system manages this content and many other aspects.

The filtering system:

- Should not be overly restrictive and inadvertently block acceptable content;
- should be deployed such that it cannot be easily circumvented by the user, and mitigates technologies and techniques used to circumvent the system, for example VPNs, proxy services and DNS over HTTPS.
- Should have a process to whitelist sites that are blocked.

Desirable requirement:

- Recognising the requirement for the device to be safe to use “out of the box” for any user, it is desirable that the filtering solution can be configured for age appropriate filtering for different groups of users, e.g. by key stages and school staff.

- Static url block/allow lists alone will not provide the highest level of protection and look to bidders to propose a solution that shall dynamically check content using methods such as keyword filtering to prevent inappropriate access.

Security

The devices shall be configured using a baseline developed using, where appropriate to the nature of the deployment, the Cyber Essentials control areas and the NCSC EUD and Mobile Device guidance. This shall include, at a minimum:

- Protection from malicious actors and other security risks including malware (and ransomware) while also minimising the impact of phishing,
- Security software shall be updated on a regular basis to keep the device protected from the latest risks.
- Data at rest on the device shall be protected by the encryption built into the platforms.
- The device shall be configured to prevent the end user from downloading and installing applications with the exception of legitimate operating system updates and security patches, or other required software distributed through the app stores available by default on the device.
- Online accounts used for administration of the filtering system, and any other device administration/security systems shall be protected by multi-factor authentication, ideally using FIDO-compliant hardware keys where these are compatible with the service. Actions by administrators shall also be auditable by the other administrators and the number of highest privilege users reduced to the minimum necessary (with lower privileged user roles utilised for performing day-to-day administration).

ON-BOARDING AND SUPPORT THROUGHOUT THE LIFE OF THE CONTRACT

The Buyer requires a dedicated customer success manager (CSM). The CSM shall be assigned for the duration of the Contract. The CSM role will focus on project management activities, managing any queries/issues, and ensuring the Buyer and Responsible Bodies are kept abreast of and benefiting from all the capabilities of the product. The CSM will be responsible for the preparation and delivery of customer Service reviews.