Digital Outcomes and Specialists 5 (RM1043.7)

Framework Schedule 6 (Order Form)

Version 2

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Order Form

Call-Off Reference: **CCTS22A98**

Call-Off Title: **Provision of Domain Management (Requirement 2)**

Call-Off Contract Description: **Small Organisation Helper Service – to help Parish Councils adopt gov.uk domains securely**

The Buyer: **Cabinet Office**

Buyer Address: **REDACTED TEXT under FOIA Section 40, Personal Information**

The Supplier: **CMC Partnership Consultancy Ltd**

Supplier Address: **Excalibur House, Priory Drive, Newport, NP18 2HJ**

Registration Number: **11458998**

DUNS Number: **REDACTED TEXT under FOIA Section 40, Personal Information**

SID4GOV ID: **REDACTED TEXT under FOIA Section 40, Personal Information**

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Applicable Framework Contract

This Order Form is for the provision of the Call-Off Deliverables and dated 15th March 2023.

It's issued under the Framework Contract with the reference number RM1043.7 for the provision of Digital Outcomes and Specialists Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first Statement of Work which shall be executed at the same time that the Call-Off Contract is executed, oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

Call-Off Lot

Lot 1 – Digital Outcomes.

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) RM1043.7

3 Framework Special Terms

4 The following Schedules in equal order of precedence:

- Joint Schedules for RM1043.7
    - 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) RM1043.7

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

- Call-Off Schedules for RM1043.7
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 2 (Staff Transfer)
    - Call-Off Schedule 3 (Continuous Improvement)
    - Call-Off Schedule 5 (Pricing Details and Expenses Policy)
    - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)
    - 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 13 (Implementation Plan and Testing)
    - Call-Off Schedule 18 (Background Checks)
    - Call-Off Schedule 20 (Call-Off Specification)
    - Call-Off Schedule 26 (Cyber Essentials Scheme)

5 CCS Core Terms (version 3.0.9)

6 Joint Schedule 5 (Corporate Social Responsibility) RM1043.7

7 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

8 The Buyer's additional security schedule as outlined in Annex 2 of this Order Form.

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

Call-Off Special Terms

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

None.

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Call-Off Start Date: **20th March 2023**

Call-Off Expiry Date: **19th September 2023**

Call-Off Initial Period: **Six (6) months**

Call-Off Optional Extension Period: **Three (3) months**

Minimum Notice Period for Extensions: **One (1) month**

Call-Off Contract Value: **£224,700.00. This does not include any extension periods and is excluding VAT.**

Call-Off Deliverables

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

Buyer's Standards

From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards referred to in Framework Schedule 1 (Specification). The Buyer requires the Supplier to comply with the following additional Standards for this Call-Off Contract:

Not applicable.

Cyber Essentials Scheme

The Buyer requires the Supplier, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme) to provide a Cyber Essentials Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

Maximum Liability

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms as amended by the Framework Award Form Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £224,700.00 (excluding VAT).

Call-Off Charges

Fixed Price.

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, and the Supplier shall, under each SOW, charge the Buyer a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

Reimbursable Expenses

None.

Payment Method

BACs.

Buyer's Invoice Address

REDACTED TEXT under FOIA Section 40, Personal Information

Buyer's Authorised Representative

REDACTED TEXT under FOIA Section 40, Personal Information

Buyer's Environmental Policy

Not applicable.

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Buyer's Security Policy

Appended at Call-Off Schedule 9 (Security) and Annex 2 – Additional Security Schedule.

Supplier's Authorised Representative

REDACTED TEXT under FOIA Section 40, Personal Information

Supplier's Contract Manager

REDACTED TEXT under FOIA Section 40, Personal Information

Progress Report Frequency

Fortnightly in alignment with the Contracting Authority's sprints

Progress Meeting Frequency

Fortnightly in alignment with the Contracting Authority's sprints

Key Staff

REDACTED TEXT under FOIA Section 40, Personal Information

Key Subcontractor(s)

Not applicable

Commercially Sensitive Information

The supplier's technical submission and commercial proposal.

Balanced Scorecard

Not applicable.

Material KPIs

The following KPIs, as outlined in Call-Off Schedule 20 Specification, shall apply to this contract:

- Reduce the time that domain-related vulnerabilities are open for exploitation, and hence reduce the government's exposure to risk;
- Increase the ability of registrars to address the support needs of Parish Councils;
- Improves awareness and skills around domain management;
- Increase adoption of .gov.uk domains and modern cloud services across Parish Councils;
- Lead to better incident response and preparation for future potential incidents;
- Lead to a reduced workload for the CDDO team;
- Lead to a consistent security approach for domains when being used across more than one organisation.

Additional Insurances

Not applicable.

Guarantee

Not applicable.

Social Value Commitment

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender).

Statement of Works

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute

completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

For and on behalf of the Supplier:
REDACTED TEXT under FOIA Section 40, Personal Information

For and on behalf of the Buyer:
REDACTED TEXT under FOIA Section 40, Personal Information

Appendix 1

The first Statement(s) of Works shall be inserted into this Appendix 1 as part of the executed Order Form. Thereafter, the Buyer and Supplier shall complete and execute Statement of Works (in the form of the template Statement of Work in Annex 1 to the template Order Form in Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules).

Annex 1 (Template Statement of Work)

1 Statement of Works (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.

All SOWs must fall within the Specification and provisions of the Call-Off Contact.

The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.

Date of SOW: 15th March 2023

SOW Title: Small Organisation Helper Service

SOW Reference: CCTS22A98

Call-Off Contract Reference: CCTS22A98

Buyer: Cabinet Office

Supplier: CMC Partnership Consultancy Ltd

SOW Start Date: 15th March 2023

SOW End Date: 14th September 2023

Duration of SOW: Full duration of the contract, including any extension options.

Key Personnel (Buyer):
REDACTED TEXT under FOIA Section 40, Personal Information
Key Personnel (Supplier):
REDACTED TEXT under FOIA Section 40, Personal Information

Subcontractors:

N/A.

Call-Off Contract Specification – Deliverables Context

SOW Deliverables Background: All elements of deliverables shall be addressed by this SOW.

Delivery phase(s): Discovery and Pilot phase.

Overview of Requirement:

Why the work is being done

CDDO wishes to increase the adoption and secure use of '.gov.uk' domains and modern cloud services linked to these domains across English Parish Councils, Parish Meetings, and small Town Councils. This would bring a step change in the country's cyber resilience at the foundational tier of our democracy because '.gov.uk' domains are continuously monitored, and if they get subverted for malicious purposes this will be quickly spotted.

Of approximately 3,500 third-level ".gov.uk" domains, around 1800 have been registered with Parish Councils.

There are over 10,000 PC's in total, so many have chosen either to use a non-government domain, or not to have a domain at all. This may be because:

- It's hard for someone unfamiliar with current best security practice to know where to start to guard against, or help others to guard against the most common cyber threats

- there are obligations that come with having a .gov.uk domain and it's difficult to discharge these obligations without knowledgeable IT support

This procurement is just for the Discovery and Pilot phase of this project. Future phases (alpha, beta, and live) will be subject to approvals, funding, and the successful delivery of this Discovery and Pilot phase.

Problem to be solved

Work with NALC/SLCC to recruit 5 PCs who don't have a .gov.uk domain plus 5 PCs who do have a .gov.uk domain but finding it difficult to adopt it.

Conduct user research and business analysis with each PC to identify barriers that exist for them to adopt a .gov.uk domain and modern cloud services.

Work through CDDO/above bodies to recruit 10 .gov.uk domain registrars that provide services to PCs at different scales. The PC's registrars must be included.

Conduct user research and business analysis with these registrars to understand support models they currently offer, and how they can be adapted to deliver the outcome.

Define and trial its proposed methods to improve adoption and its pilot support model, with all participants in this discovery and pilot phase.

Deliver:

- User research and business analysis notes from all engagements.
- A draft proposal for new ways of working, including:
    - scalable methods for improving .gov.uk adoption by PCs
    - changes to the support model provided by domain registrars to PCs
- The new ways of working deployed across all the PCs/registrars involved in the Pilot phase.
- A detailed review of how successful these new ways of working are, and any recommendations.
- KPI definitions/data to baseline progress.

Who the users are and what they need to do

As a Clerk to a Parish Council, I need:

- my Parish to have a .gov.uk domain so that we can get the benefits of having a .gov.uk domain.

- my Parish to have its IT services set up with a .gov.uk domain so that we can get the benefits of having a .gov.uk domain.

- access to training and support so that my Parish Councillors and I can use our .gov.uk domain on our personal IT.

As a Parish Councillor, I need

- to understand what the benefits of having a .gov.uk domain are and why I should use it.

- to have my personal IT configured properly so that I can use my .gov.uk domain for my parish business.

- to know how to use my .gov.uk domain on my personal IT so that I can use my .gov.uk domain for my parish email.

- to use my .gov.uk domain on my personal IT so that my Parish and I can get the benefits of having a .gov.uk domain.

See:
https://www.gov.uk/guidance/benefits-of-getting-a-govuk-domain?step-by-step-nav=5a9309a3-9a80-4faa-b24f-1797023e897f

2 Buyer Requirements – SOW Deliverables

Outcome Description:

Milestone Ref	Milestone Description	Acceptance Criteria	Due Date
MS01	The supplier must work with the National Association of Local Councils, County Associations and the Society of Local Council Clerks to recruit 5 Parish Councils who don't have a .gov.uk domain plus 5 Parish Councils who do have a .gov.uk domain but are finding it difficult to adopt it.	All elements of milestone description delivered	Month 1
MS02	The supplier must conduct user research and business analysis with the Clerk and at least 1 Councillor in each Parish Council to identify the	All elements of milestone description delivered	Month 4

	specific barriers that exist for them to adopting a .gov.uk domain and modern cloud services.		
MS03	The supplier must work through CDDO or the above bodies to recruit 10 .gov.uk domain registrars that provide services to Parish councils at different scales. The registrars of the recruited Parish Councils must be included.	All elements of milestone description delivered	Month 4
MS04	The supplier must conduct user research and business analysis with these registrars to understand the support models they currently offer, and how they can be adapted to deliver the outcome.	All elements of milestone description delivered	Month 4
MS05	The supplier must define and trial its proposed methods to improve adoption and its pilot support model, with all the participants in this discovery and pilot phase.	All elements of milestone description delivered	Month 4
MS06	User research and business analysis interview notes from all engagements.	All elements of milestone description delivered	Month 5
MS07	Changes to the support model provided by domain registrars to Parish Councils.	All elements of milestone description delivered	Month 5
MS08	The new ways of working deployed across all the Parish Councils and registrars involved in the Pilot phase.	All elements of milestone description delivered	Month 6
MS09	A detailed review how successful these new ways of working are, and any recommendations for changes.	All elements of milestone description delivered	Month 6
MS10	KPI definitions and initial KPI data to baseline progress towards achieving the outcome and goal.	All elements of milestone description delivered	Month 6

Delivery Plan: As outlined in the table above.

Dependencies: Central Digital and Data Office (CDDO) will provide all necessary domains vulnerability information. The data will be accessible only to those who are authorised to receive it.

Supplier Resource Plan:

Name	Role	Main responsibilities
REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information
REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information
REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information
REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information

All team members will be engaged for the full duration of the assignment.

Security Applicable to SOW:

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security). The Supplier confirms that they shall adhere to Appendix 2 – Additional security schedule as outlined in this Order Form.

Cyber Essentials Scheme:

The Buyer requires the Supplier to have and maintain a **Cyber Essentials Certificate** for the work undertaken under this SOW, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme).

SOW Standards:

The supplier must follow the Service Manual to deliver this project. The supplier must achieve a successful service assessment if required.

Performance Management:

Material KPIs	Target	Measured by
Reduce the time that domain-related vulnerabilities are open for exploitation, and hence reduce the government's exposure to risk.	The targets will be agreed during the engagement	Supplier delivery of milestones as outlined in section 3.
Increase the ability of registrars to address the support needs of Parish Councils.	The targets will be agreed during the engagement	Supplier delivery of milestones as outlined in section 3.
Improves awareness and skills around domain management.	The targets will be agreed during the engagement	Supplier delivery of milestones as outlined in section 3.
Increase adoption of .gov.uk domains and modern cloud services across Parish Councils.	The targets will be agreed during the engagement	Supplier delivery of milestones as outlined in section 3.
Lead to better incident response and preparation for future potential incidents.	The targets will be agreed during the engagement	Supplier delivery of milestones as outlined in section 3.
Lead to a consistent security approach for domains when being used across more than one organisation.	The targets will be agreed during the engagement	Supplier delivery of milestones as outlined in section 3.

Additional Requirements:

Annex 1 – Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex 1 attached to this Statement of Work.

Key Supplier Staff:

Key Role	Key Staff	Contract Details	Employment / Engagement Route (incl. inside/outside IR35)
REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information

REDACTED TEXT under FOIA Section 40, Personal Information	**REDACTED TEXT under FOIA Section 40, Personal Information**	**REDACTED TEXT under FOIA Section 40, Personal Information**	**REDACTED TEXT under FOIA Section 40, Personal Information**

REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information
REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information

SOW Reporting Requirements:

Fortnightly in alignment with the Contracting Authority's sprints.

3 Charges

Call Off Contract Charges:

The applicable charging method(s) for this SOW is:

- Fixed Price.

The estimated maximum value of this SOW (irrespective of the selected charging method) is £224,700.00 (excluding VAT). This is not including any extension options to the contract duration.

Reimbursable Expenses:

None.

Signatures and Approvals

Agreement of this SOW

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

For and on behalf of the Supplier

REDACTED TEXT under FOIA Section 40, Personal Information

For and on behalf of the Buyer

REDACTED TEXT under FOIA Section 40, Personal Information

Annex 1

Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 do not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

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 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: • All data associated with this agreement **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • Business contact details of Supplier Personnel for which the Supplier is the Controller, • Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller
Duration of the Processing	The full duration of the contract
Nature and purposes of the Processing	Data will be collected for the purposes of: • user research • customer outreach The nature of this processing could be any of the following: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation
Type of Personal Data	This includes full name, work email address, work phone, role and organisation

Categories of Data Subject	Staff in other government departments and the wider public sector and domain registrars
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 will undertake this work on the CDDO enterprise network using tools and platforms provided and agreed by the CDDO and in compliance with the Cabinet Office data protection framework The data will be processed and retained by the Supplier only for the duration of this contract and will be completely destroyed and all copies returned to the Relevant Authority.

Appendix 2 – Additional Security Schedule

1 Supplier obligations

Core requirements

1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 8.

1.2 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Certifications (see Paragraph 3)		
The Supplier must have the following Certifications:	ISO/IEC 27001:2013 by a recognised certification body	**X**
	Cyber Essentials Plus	☐
	Cyber Essentials	X
Subcontractors that Process Government Data must have the following Certifications:	ISO/IEC 27001:2013 by a recognised certification body	**X**
	Cyber Essentials Plus	☐
	Cyber Essentials	**X**

Locations (see Paragraph 4)		
The Supplier and Subcontractors may store, access or Process Government Data in:	the United Kingdom only	**X**
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐

Optional requirements

1.3 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

Security testing (see Paragraph 9)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	**X**
Cloud Security Principles (see Paragraph 10)	
The Supplier must assess the Supplier System against the Cloud Security Principles	**X**
Record keeping (see paragraph 11)	
The Supplier must keep records relating to Subcontractors, Sites, Third Party Tools and third parties	**X**
Encryption (see Paragraph 12)	
The Supplier must encrypt Government Data while at rest or in transit	**X**
Protecting Monitoring System (see Paragraph 13)	
The Supplier must implement an effective Protective Monitoring System	**X**
Patching (see Paragraph 14)	
The Supplier must patch vulnerabilities in the Supplier System promptly	**X**
Malware protection (see Paragraph 15)	
The Supplier must use appropriate Anti-virus Software	**X**

End-user Devices (see Paragraph 16)	
The Supplier must manage End-user Devices appropriately	**X**
Vulnerability scanning (see Paragraph 17)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	**X**
Access control (see paragraph 18)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	**X**
Return and deletion of Government Data (see Paragraph 19)	
The Supplier must return or delete Government Data when requested by the Buyer	**X**
Physical security (see Paragraph 20)	
The Supplier must store Government Data in physically secure locations	**X**
Security breaches (see Paragraph 21)	
The Supplier must report any Breach of Security to the Buyer promptly	**X**
Security Management Plan (see Paragraph 22)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected have been met.	**X**

2 Definitions

"Anti-virus Software"	means software that: **(a)** protects the Supplier System from the possible introduction of Malicious Software; **(b)** scans for and identifies possible Malicious Software in the Supplier System; **(c)** if Malicious Software is detected in the Supplier System, so far as possible: **(i)** prevents the harmful effects of the Malicious Software; and **(ii)** removes the Malicious Software from the Supplier System;

"Contract Year"	means: **(a)** a period of 12 months commencing on the Effective Date; **(b)** thereafter a period of 12 months commencing on each anniversary of the Effective Date; **(c)** with the final Contract Year ending on the expiry or termination of the Term;
"CREST Service Provider"	means a company with an information security accreditation of a security operations centre qualification from CREST International;
"Government Data"	means any: **(a)** data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; **(b)** Personal Data for which the Buyer is a, or the, Data Controller; or **(c)** any meta-data relating to categories of data referred to in paragraphs (a) or (b); that is: **(d)** supplied to the Supplier by or on behalf of the Buyer; or **(e)** that the Supplier generates, processes, stores or transmits under this Agreement; and for the avoidance of doubt includes the Code and any meta-data relating to the Code.
"Certifications"	means one or more of the following certifications: **(b)** ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and **(c)** Cyber Essentials Plus; and/or **(d)** Cyber Essentials;
"Breach of Security"	means the occurrence of: **(a)** any unauthorised access to or use of the Services, the Sites, the Supplier System

	and/or the Government Data; **(b)** the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or **(c)** any part of the Supplier System ceasing to be compliant with the required Certifications; **(d)** the installation of Malicious Software in the Supplier System: **(e)** any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and **(f)** includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: **(i)** was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or **(ii)** was undertaken, or directed by, a state other than the United Kingdom;
"CHECK Scheme"	means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
"CHECK Service Provider"	means a company which, under the CHECK Scheme: **(a)** has been certified by the NCSC; **(b)** holds "Green Light" status; and **(c)** is authorised to provide the IT Health Check services required by Paragraph 5.2 (*Security Testing*);
"Cloud Security Principles"	means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles.
"Cyber	means the Cyber Essentials certificate issued under the

Essentials"	Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the NCSC;
"End-user Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
"IT Health Check"	means testing of the Supplier Information Management System by a CHECK Service Provider;
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC"	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"Privileged User"	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
"Process"	means any operation performed on data, whether or not by automated means, including 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 that data;
"Prohibition Notice"	means the meaning given to that term by Paragraph 4.4.
"Protective Monitoring System"	has the meaning given to that term by Paragraph 13.1;
"Relevant	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the

Conviction"	Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
"Sites"	means any premises (including the Buyer's Premises, the Supplier's premises or third party premises): **(a)** from, to or at which: **(i)** the Services are (or are to be) provided; or **(ii)** the Supplier manages, organises or otherwise directs the provision or the use of the Services; or **(b)** where: **(i)** any part of the Supplier System is situated; or **(ii)** any physical interface with the Authority System takes place;
"Standard Contractual Clauses" **(replaced by International Data Transfer Agreements (IDTA"s) from Sept 22)**	means, for the purposes of this Schedule (*Security Management*): **(a)** the standard data protection paragraphs specified in Article 46 of the UK GDPR setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area; **(b)** as modified to apply equally to the Government Data as if the Government Data were Personal Data;
"Subcontractor Personnel"	means: **(a)** any individual engaged, directly or indirectly, or employed, by any Subcontractor; and **(b)** engaged in or likely to be engaged in: **(i)** the performance or management of the Services; or **(ii)** the provision of facilities or services that are necessary for the provision of the Services;
"Supplier System"	means **(a)** any:

	(i) information assets, **(ii)** IT systems, **(iii)** IT services; or **(iv)** Sites, that the Supplier or any Subcontractor will use to Process, or support the Processing of, Government Data and provide, or support the provision of, the Services; and **(b)** the associated information management system, including all relevant: **(i)** organisational structure diagrams; **(ii)** controls; **(iii)** policies; **(iv)** practices; **(v)** procedures; **(vi)** processes; and **(vii)** resources;
"Third-party Tool"	means any activity conducted other than by the Supplier during which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;

Part One: Core Requirements

3 Certification Requirements

3.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Process Government Data are certified as compliant with Cyber Essentials.

3.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

(a) it; and

(b) any Subcontractor that Processes Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1:

3.3 The Supplier must ensure that the specified Certifications are in place for it and any relevant Subcontractor:

(a) before the Supplier or any Subcontractor Processes Government Data; and

(b) throughout the Term.

4 Location

4.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or

Process Government Data outside the United Kingdom.

4.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that its Subcontractors, at all times store, access or process Government Data only in or from the geographic areas specified by the Buyer.

4.3 Where the Buyer has permitted the Supplier and its Subcontractors to store, access or process Government Data outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Subcontractors store, access or process Government Data in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);

(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);

(c) the Supplier or Subcontractor has taken reasonable steps to assure itself that:

(i) the entity complies with the binding agreement; and

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule (*Security Management*);

(d) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 4.4.

4.4 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken the storage, accessing or Processing of Government Data in one or more countries or territories (a "**Prohibition Notice**").

4.5 Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

5 Staff vetting

5.1 The Supplier must not allow Supplier Personnel, and must ensure that Subcontractors do not allow Subcontractor Personnel, to access or Process Government Data, if that person:

(a) has not completed the Staff Vetting Procedure; or

(b) where no Staff Vetting Procedure is specified in the Order Form:

(i) has not undergone the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

(A) the individual's identity;

(B) where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United

Kingdom; and

(C) the individual's previous employment history; and

(D) that the individual has no Relevant Convictions; and

(ii) has not undergone national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify

6 Supplier assurance letter

6.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its chief technology officer (or equivalent officer) confirming that, having made due and careful enquiry:

(a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Agreement;

(b) it has fully complied with all requirements of this Schedule (Security Management); and

(c) all Subcontractors have complied with the requirements of this Schedule (Security Management) with which the Supplier is required to ensure they comply;

(d) the Supplier considers that its security and risk mitigation procedures remain effective.

7 Assurance

7.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Schedule (*Security Management*).

7.2 The Supplier must provide that information and those documents:

(a) within 10 Working Days of a request by the Buyer;

(b) except in the case of original document, in the format and with the content and information required by the Buyer; and

(c) in the case of original document, as a full, unedited and unredacted copy.

8 Use of Subcontractors and third parties

8.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Process Government Data comply with the requirements of this Schedule (Security Management).

Part Two: Additional Requirements

9 Security testing

9.1 The Supplier must:

(a) before Processing Government Data;

(b) at least once during each Contract Year; and

undertake the following activities:

(c) conduct security testing of the Supplier System (an "**IT Health Check**") in accordance with Paragraph 9.2; and

(d) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 9.3.

9.2 In arranging an IT Health Check, the Supplier must:

(a) use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

(b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

(c) ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Process or manage Government Data; and

(d) ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

9.3 The Supplier treat any vulnerabilities as follows:

(a) the Supplier must remedy any vulnerabilities classified as critical in the IT Health Check report:

(i) if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(a)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(b) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

(i) if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(c) the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

(i) if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(d) where it is not technically feasible to remedy the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

10 Cloud Security Principles

10.1 The Supplier must ensure that the Supplier Solution complies with the Cloud Security Principles.

10.2 The Supplier must assess the Supplier Solution against the Cloud Security Principles to assure itself that it complies with Paragraph 10.1:

(a) before Processing Government Data;

(b) at least once each Contract Year; and

(c) when required by the Buyer.

10.3 The Supplier must:

(a) keep records of any assessment that it makes under Paragraph 10.2; and

(b) provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

11 Information about Subcontractors, Sites, Third Party Tools and third parties

11.1 The Supplier must keep the following records:

(a) for Subcontractors or third parties that store, have access to or Process Government Data:

(i) the Subcontractor or third party's name:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual), including:

(1) country of registration;

(2) registration number (if applicable); and

(3) registered address;

(ii) the Relevant Certifications held by the Subcontractor or third party;

(iii) the Sites used by the Subcontractor or third party;

(iv) the Services provided or activities undertaken by the Subcontractor or third party;

(v) the access the Subcontractor or third party has to the Supplier System;

(vi) the Government Data Processed by the Subcontractor or third party; and

(vii) the measures the Subcontractor or third party has in place to comply with the requirements of this Schedule (*Security Management*);

(b) for Sites from or at which Government Data is accessed or Processed:

(i) the location of the Site;

(ii) the operator of the Site, including the operator's:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual);

(iii) the Relevant Certifications that apply to the Site;

(iv) the Government Data stored at, or Processed from, the site; and

(c) for Third Party Tools:

(i) the name of the Third Party Tool;

(ii) the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and

(iii) in respect of the entity providing the Third-Party Tool, its:

(A) full legal name;

(B) trading name (if any)

(C) country of registration;

(D) registration number (if applicable); and

(E) registered address.

11.2 The Supplier must update the records it keeps in accordance with Paragraph 11.1:

(a) at least four times each Contract Year;

(b) whenever a Subcontractor, third party that accesses or Processes Government Data, Third Party Tool or Site changes; or

(c) whenever required to go so by the Buyer.

11.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 11.1 to the Buyer within 10 Working Days of any request by the Buyer.

12 Encryption

12.1 The Supplier must, and must ensure that all Subcontractors, encrypt Government Data:

(a) when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

(b) when transmitted.

13 Protective monitoring system

13.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

(a) identify and prevent any potential Breach of Security;

(b) respond effectively and in a timely manner to any Breach of Security that does;

(c) identify and implement changes to the Supplier System to prevent future any Breach of Security; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

(the "**Protective Monitoring System**").

13.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier System; and

(b) regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Government Data; and

(c) the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

14 Patching

14.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

(a) the Supplier must patch any vulnerabilities classified as "critical":

(i) if it is technically feasible to do so, within 5 Working Days of the public release; or

(ii) if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(a)(i), then as soon as reasonably practicable after the public release;

(b) the Supplier must patch any vulnerabilities classified as "important":

(i) if it is technically feasible to do so, within 1 month of the public release; or

(ii) if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(b)(i), then as soon as reasonably practicable after the public release;

(c) the Supplier must remedy any vulnerabilities classified as "other" in the public release:

(i) if it is technically feasible to do so, within 2 months of the public release; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 14.1(c)(i), then as soon as reasonably practicable after the public release;

(d) where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

15 Malware protection

15.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

15.2 The Supplier must ensure that such Anti-virus Software:

(a) prevents the installation of the most common forms of Malicious Software in the Supplier System;

(b) performs regular scans of the Supplier System to check for Malicious Software; and

(c) where Malicious Software has been introduced into the Supplier System, so far as practicable

(i) prevents the harmful effects from the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System.

16 End-user Devices

16.1 The Supplier must, and must ensure that all Subcontractors, manage all End-user Devices on which Government Data is stored or processed in accordance with the following requirements:

(a) the operating system and any applications that store, process or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Government Data must be encrypted using a suitable encryption tool;

(d) the End-under Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;

(f) the Suppler or Subcontractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Government Data stored on the device and prevent any user or group of users from accessing the device;

(g) all End-user Devices are within the scope of any required Certification.

16.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

17 Vulnerability scanning

17.1 The Supplier must:

(a) scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

(b) if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 14.

18 Access control

18.1 The Supplier must, and must ensure that all Subcontractors:

(a) identify and authenticate all persons who access the Supplier System before they do so;

(b) require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

(c) allow access only to those parts of the Supplier System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier System.

18.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End-user Devices;

(c) are configured so that those accounts can only be used for system administration tasks;

(d) require passwords with high complexity that are changed regularly;

(e) automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and

(f) are:

(i) restricted to a single role or small number of roles;

(ii) time limited; and

(iii) restrict the Privileged User's access to the internet.

19 Return and deletion of Government Data

19.1 When requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

(a) securely erase any or all Government Data held by the Supplier or Subcontractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

(b) provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor using the method specified by the Buyer.

20 Physical security

20.1 The Supplier must, and must ensure that Subcontractors, store the

Government Data on servers housed in physically secure locations.

21 Breach of security

21.1 If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

(a) notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours.

(b) provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction.

(c) where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer.

22 Security Management Plan

22.1 This Paragraph 22 applies only where the Buyer has selected this option in paragraph 1.3.

Preparation of Security Management Plan

22.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule (*Security Management*) and the Agreement in order to ensure the security of the Supplier solution and the Buyer data.

22.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Agreement, the Security Management Plan, which must include a description of how all the options selected in this schedule are being met along with evidence of the required certifications for the Supplier and any Subcontractors specified in Paragraph 3.

Approval of Security Management Plan

22.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

(a) an information security approval statement, which shall confirm that the Supplier may operate the service and process Buyer data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

22.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

22.6 The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

Updating Security Management Plan

22.7 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required

by this Paragraph.

Monitoring

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

(a) a significant change to the components or architecture of the Supplier Information Management System;

(b) a new risk to the components or architecture of the Supplier Information Management System;

(c) a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

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

(h) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval