DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	ECM_10003
THE BUYER:	Department of Work and Pensions (DWP)
BUYER ADDRESS	Caxton House Tothill Street London SW1H 9NA
THE SUPPLIER:	Commissum Associates Limited
SUPPLIER ADDRESS:	Zone 3, First Floor Office Suite, 5 Mitchell Street, Edinburgh, Scotland, EH6 7BD
REGISTRATION NUMBER:	SC229945
DUNS NUMBER:	
DPS SUPPLIER REGISTRATION SERVICE ID:	

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 29/04/2022.
It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
NCSC Assured Services, Penetration Testing/Pen test, IT Health Check, Clearance: Security Check, Government

ORDER INCORPORATED TERMS
The following documents are incorporated into this Order 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 Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:
   - Joint Schedules for RM3764iii
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)
     - Joint Schedule 4 (Commercially Sensitive Information)

   - Order Schedules for RM3764iii
     - Order Schedule 4 (Order Tender)
     - Order Schedule 8 (Business Continuity and Disaster Recovery)
     - Order Schedule 9 (Security)
     - Order Schedule 10 (Exit Management)
     - Order Schedule 14 (Service Levels)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Appendix 1 – Security Level Requirements Level 1 and 2

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

ORDER SPECIAL TERMS

DWP has legal and regulatory obligations to verify that the suppliers we work with have a reasonable standard of security in place to protect Authority data and assets. DWP is committed to the protection of its information, assets and personnel and expects the same level of commitment from its suppliers (and sub-contractors if applicable). In order to protect the Department appropriately, DWP have recently reviewed its Security Supplier Assurance process and requirements and have made the applicable changes in line with industry good practice.

These changes include but are not limited to:

- Updated 'Security Schedule'.
- Replacement of 'Security Management Plans' with the completion of the 'Information Security Questionnaire' as part of the tender submission.
- Compliance with the DWP's relevant policies and standards, found at gov.uk.
- Compliance to industry good practice such as 'ISO27001' and certification to 'Cyber Essentials'.

Full information about DWP's security safeguards and requirements can be found in the DWP Security Schedule at Appendix 1 – Security Level Requirements Level 1 and 2.

ORDER START DATE: 29th April 2022

ORDER EXPIRY DATE: 28th April 2023

ORDER INITIAL PERIOD: 12 months

ORDER OPTIONAL EXTENSION: This Order Form can be extended by the Buyer for two periods of up to twelve months, by giving the Supplier one month's written notice before its expiry. The estimated cost for each twelve-month extension period(s) is £440,210 excluding VAT.

DELIVERABLES

This Order Contract will be delivered in line with the Suppliers proposal below: -

[Redacted]

This Order Contract is for the Service, with outcome-based deliverables detailed in the table below and will be operated as follows:

This contract is for a service, with outcome-based deliverables detailed in the table below and will be operated as follows:

- The Supplier Staff will be under the day to day direction and control of the Supplier, not DWP;
- Any quality and non-delivery issues will be raised by DWP directly with the supplier rather than the individual Supplier Staff;
- The Supplier will be held accountable by DWP for non-delivery of the Services that are specified in this contract, not the individual Supplier Staff;
- The Supplier is able to substitute the individual Supplier Staff to undertake the Services within this contract.
- This contract will not be used to fill roles that already exist in DWP

#	Deliverable / Outcome	Details of Activities	Outputs / Acceptance criteria	Estimated Milestone Date	Milestone #
D1	Security technical assurance	• Deliver continuous PEN testing/vulnerability assessments of existing and new features within DWP application services • Support work to automate security	The supplier must log relevant pen test findings as tickets on DWP's JIRA application (Supplier will endeavour to log within 72 hours of identification. Critical findings, as per CVSS scoring, must be alerted verbally to DWP at the immediate conclusion of any test and logged within 12 business hours of being discovered). If the supplier in the course of activities identifies a security incident this	Ongoing – 28/04/2023	N/A

		testing within a CI/CD environment. • Provision of specific security inspired insight and technical assurance – responding to current security threats and vulnerabilities. • Performance of bespoke security testing during iterative development stages. • Deployment of automated testing tools and training of DWP staff and contractors in their use. • Production and delivering of security test scripts. • Provision of consultancy for hardening, secure coding and vulnerability management. • Scope / validate external IT health checks	must be reported immediately as per DWP Security Incident process. DWP Delivery manager to validate invoice against JIRA tickets raised and confirm satisfaction and acceptance of deliverable ahead of sign off / approval for payment. Documentation to include deployment guides and configuration documentation, short form report documentation, completion of Wiki's Training materials to include videos, slides, handbooks, links and other reference materials Supplier will provide representation at DWP meetings as required		
Deliverables D2 – D4 are linked to a discovery phase and the output will lead to a DWP decision as to which recommendations can be adopted and will be implemented.					
D2	OWASP SAMM 2.0 assessment, maturity model report	• Supplier to complete SAMM 2.0 assessment, maturity model report and 12-month roadmap	Completed reports and roadmap presented to DWP Delivery Manager	17/06/2022	1

	and 12-month roadmap				
D3	Support to train DWP staff to do additional SAMM 2.0 assessments	• Supplier to provide consultancy / training to DWP • Supplier to validate and provide comments for SAMM 2.0 assessments completed by DWP	Training sessions to be recorded Completed and validated SAMM 2.0 assessments presented to DWP Delivery Manager	22/07/2022	1
D4	Combining SAMM assessments from different DWP teams	• Supplier and DWP to review and compare outputs from Deliverable D3	Supplier to provide written PDF management report with findings to DWP Delivery Manager	29/07/2022	1
The output from the SAMM 2.0 assessments will be presented to DWP with a prioritisation matrix and DWP will decide which recommendations can be adopted and implemented. If DWP decide not to proceed with any recommendations, then Deliverables D5 – D7 (implementation) will not be required. Deliverable D1 & D8 will continue throughout the Order Form Contract duration.					
D5	Engineering support to deploy tooling, configure, test, and run initial scans and test scripts	• Supplier and DWP to agree which tools are to be deployed based on the output from Deliverable D4 • Supplier and DWP to agree success criteria • Supplier to ensure tools are configured and working correctly	Supplier to provide copies of test scripts for tools deployed to DWP Delivery Manager Tools are successfully deployed and working and signed off by DWP Delivery Manager	30/09/2022	2

D6	Engineering support to manage the test tooling containers and other infrastructure	Supply hands on engineering to do set up and provide ongoing support via CI/CD pipeline	Supplier to provide: • Infrastructure-as-code • Containers • Deployment manifests • CI/CD pipelines • Infrastructure code repositories	30/09/2022 - 28/04/2023	2
D7	Knowledge transfer	Supplier to provide training materials / knowledge transfer documentation	Supplier to provide training / knowledge transfer documentation	30/09/2022 – 28/04/2023	3
D8	Debrief report	Supplier to provide debrief report to DWP and handover notes and documentation	Final debrief report, including lessons learnt, presented to DWP Delivery Manager	2- 3 weeks before end of contract	4

ASSUMPTIONS / DEPENDENCIES

- DWP team will support completing SAMM assessments in good time as well as provide any engineering support to deploy tooling
- DWP to provide subject matter expert representation at meetings to provide input, feedback and approval as required
- DWP's pipelines and developer environment are able to support security test automation
- DWP will invest in allowing developers and non-functional testers the space and time to learn to run and interpret security tooling.

MAXIMUM LIABILITY

The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms. The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £440,210 excluding VAT (Estimated Charges in the first 12 months of the Contract).

ORDER CHARGES

The maximum invoiceable value for this Order Contract is stated below and is subject to delivery of agreed outputs being achieved: -

Service item	Total Cost (excl. VAT)
UC: Security Vulnerability Assessment and Advice	£440,210

If full/satisfactory delivery of agreed outputs is not achieved, full payment will be withheld until acceptance criteria is met.

For transparency Deliverables D1 & D8 will be calculated based on the following charges: -

Role	Day Rate
Technical Assurance Consultant	**[Redacted]**

Discovery & Implementation phases:

Deliverable #	**Milestone #**	**Maximum Working Days**	**Day Rate**	**Maximum Cost**
D2	1	**[Redacted]**	**[Redacted]**	**[Redacted]**
D3	1	**[Redacted]**	**[Redacted]**	**[Redacted]**
D4	1	**[Redacted]**	**[Redacted]**	**[Redacted]**
D5*	2	**[Redacted]**	**[Redacted]**	**[Redacted]**
D6	2	**[Redacted]**	**[Redacted]**	**[Redacted]**
D7	3	**[Redacted]**	**[Redacted]**	**[Redacted]**
		[Redacted]		**[Redacted]**

* The output from the SAMM 2.0 assessments will be presented to DWP with a prioritisation matrix and DWP will decide which recommendations can be adopted and implemented. If DWP decide not to proceed with any recommendations then Deliverables D5 – D7 (implementation) will not be required.

The maximum invoiceable fee value at any point in time is the sum of the values associated with each of the output / acceptance criteria being met.

The full total of the above output values is: £440,210 excluding VAT.

REIMBURSABLE EXPENSES

Base location for this work is DWP Hubs in Leeds, Manchester and London and travel to these locations is included within the total Order Contract value.

PAYMENT METHOD

The payment method for this Order Contract is Purchase Order, electronic invoice and BACS payment

BUYER'S INVOICE ADDRESS:

Electronic Invoices (attached to emails) should be sent to:
APinvoices-DWP-U@gov.sscl.com

Paper invoices should be sent to:
SSCL,
PO Box 406,
Phoenix House,
Celtic Springs,
Newport
NP10 8FZ
A copy should also be emailed to: invoicing.technology-csmt@dwp.gov.uk

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

BUYER'S AUTHORISED REPRESENTATIVE

Name: **[Redacted]**
Job Title: **[Redacted]**
Email: **[Redacted]**
Address: **[Redacted]**

BUYERS CONTRACT MANAGER

Name: **[Redacted]**
Job Title: **[Redacted]**
Email: **[Redacted]**
Address: **[Redacted]**

BUYER'S ENVIRONMENTAL POLICY
Not applicable

BUYER'S SECURITY POLICY
https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards

SUPPLIER'S AUTHORISED REPRESENTATIVE

Name: **[Redacted]**
Job Title: **[Redacted]**
Email: **[Redacted]**
Address: **[Redacted]**

SUPPLIER'S CONTRACT MANAGER

Name: **[Redacted]**

Job Title: **[Redacted]**
Email: **[Redacted]**
Address: **[Redacted]**

PROGRESS REPORT FREQUENCY
Not applicable

PROGRESS MEETING FREQUENCY
Monthly Service Review Meeting and any other meetings to be agreed by both parties within 30 days of contract signature

KEY STAFF
Not applicable

KEY SUBCONTRACTOR(S)
Not applicable

COMMERCIALLY SENSITIVE INFORMATION
Supplier's pricing and/or any Supplier specific solution(s) for the period of the Order Form Term

SERVICE CREDITS
As per Order Schedule 14 (Service Levels)

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Tender)

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:	29/04/2022	Date:	29/04/2022

1. Joint Schedule 1 (Definitions)

1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.

1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In each Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings"** as references to obligations under the Contract;

1.3.8 references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract; and

1.3.12 where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

"Accreditations and Standards"	the Accreditations and Standards Filter Category detailed in DPS Schedule 1.
"Additional Insurances"	insurance requirements relating to an Order Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
"Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees;
"Affected Party"	the party seeking to claim relief in respect of a Force Majeure Event;
"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
"Annex"	extra information which supports a Schedule;
"Approval"	the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly;
"Audit"	the Relevant Authority's right to: a) verify the accuracy of the Charges and any other amounts payable by a Buyer under an Order Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) verify the Open Book Data; d) verify the Supplier's and each Subcontractor's compliance with the applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary,

	ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; k) verify the accuracy and completeness of any Management Information delivered or required by the DPS Contract;
"Auditor"	a) the Relevant Authority's internal and external auditors; b) the Relevant Authority's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office; e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and f) successors or assigns of any of the above;
"Authority"	CCS and each Buyer;
"Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer"	the relevant public sector purchaser identified as such in the Order Form;

"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Order Contract initially identified in the Order Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
"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 Order Contract;
"CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
"CCS Authorised Representative"	the representative appointed by CCS from time to time in relation to the DPS Contract initially identified in the DPS Appointment Form and subsequently on the Platform;
"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Order Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Order Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;

"Commercially Sensitive Information"	the Confidential Information listed in the DPS Appointment Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Confidential Information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
"Contract"	either the DPS Contract or the Order Contract, as the context requires;
"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"Contract Period"	the term of either a DPS Contract or Order Contract from the earlier of the: a) applicable Start Date; or b) the Effective Date until the applicable End Date;
"Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
"Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly;
"Controller"	has the meaning given to it in the GDPR;
"Core Terms"	CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under DPS Contracts and Order Contracts;

"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Man Day, of engaging the Supplier Staff, including: i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer; b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets; c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but excluding: a) Overhead; b) financing or similar costs; c) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Order Contract Period whether in relation to Supplier Assets or otherwise; d) taxation; e) fines and penalties;

	f) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Cyber Security Services"	those Service available under this DPS Contract as documented at DPS Schedule 1
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under an Order Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Levy"	has the meaning given to it in Paragraph 8.1.1 of DPS Schedule 5 (Management Levy and Information);

"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of an Order Contract as confirmed and accepted by the Buyer by confirmation in writing to the Supplier. "**Deliver**" and "**Delivered**" shall be construed accordingly;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable) for the period specified in the Order Form (for the purposes of this definition the **"Disaster Period**");
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
"Dispute"	any claim, dispute or difference arises out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as: a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables; b) is required by the Supplier in order to provide the Deliverables; and/or c) has been or shall be generated for the purpose of providing the Deliverables;
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained

	in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"DPA 2018"	the Data Protection Act 2018;
"DPS"	the dynamic purchasing system operated by CCS in accordance with Regulation 34 that this DPS Contract governs access to;
"DPS Application"	the application submitted by the Supplier to CCS and annexed to or referred to in DPS Schedule 2 (DPS Application);
"DPS Appointment Form"	the document outlining the DPS Incorporated Terms and crucial information required for the DPS Contract, to be executed by the Supplier and CCS and subsequently held on the Platform;
"DPS Contract"	the dynamic purchasing system access agreement established between CCS and the Supplier in accordance with Regulation 34 by the DPS Appointment Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;
"DPS Contract Period"	the period from the DPS Start Date until the End Date or earlier termination of the DPS Contract;
"DPS Expiry Date"	the date of the end of the DPS Contract as stated in the DPS Appointment Form;
"DPS Incorporated Terms"	the contractual terms applicable to the DPS Contract specified in the DPS Appointment Form;
"DPS Initial Period"	the initial term of the DPS Contract as specified in the DPS Appointment Form;
"DPS Optional Extension Period"	such period or periods beyond which the DPS Initial Period may be extended up to a maximum of the number of years in total specified in the DPS Appointment Form;
"DPS Pricing"	the maximum price(s) applicable to the provision of the Deliverables set out in DPS Schedule 3 (DPS Pricing);
"DPS Registration"	the registration process a Supplier undertakes when submitting its details onto the Platform;
"DPS SQ Submission"	the Supplier's selection questionnaire response;
"DPS Special Terms"	any additional terms and conditions specified in the DPS Appointment Form incorporated into the DPS Contract;
"DPS Start Date"	the date of start of the DPS Contract as stated in the DPS Appointment Form;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
"Effective Date"	the date on which the final Party has signed the Contract;

"EIR"	the Environmental Information Regulations 2004;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
"End Date"	the earlier of: a) the Expiry Date (as extended by any Extension Period exercised by the Authority under Clause 10.2); or b) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
"Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
"Estimated Year 1 Contract Charges"	the anticipated total charges payable by the Supplier in the first Contract Year specified in the Order Form;
"Estimated Yearly Charges"	means for the purposes of calculating each Party's annual liability under clause 11.2 : i) in the first Contract Year, the Estimated Year 1 Contract Charges; or ii) in any subsequent Contract Years, the Charges paid or payable in the previous Contract Year; or iii) after the end of the Contract, the Charges paid or payable in the last Contract Year during the Contract Period;
"Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
"Expiry Date"	the DPS Expiry Date or the Order Expiry Date (as the context dictates);
"Extension Period"	the DPS Optional Extension Period or the Order Optional Extension Period as the context dictates;
"Filter Categories"	the number of categories specified in DPS Schedule 1 (Specification), if applicable;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance

	and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from: a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract; b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; c) acts of a Crown Body, local government or regulatory bodies; d) fire, flood or any disaster; or e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds;
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);
"General Anti-Abuse Rule"	a) the legislation in Part 5 of the Finance Act 2013; and b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions;
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	goods made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;

"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which: i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract; or b) any Personal Data for which the Authority is the Data Controller;
"Government Procurement Card"	the Government's preferred method of purchasing and payment for low value goods or services; https://www.gov.uk/government/publications/government-procurement-card--2;
"Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HMRC"	Her Majesty's Revenue and Customs;
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including: a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the DPS Pricing/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and

	e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	the plan for provision of the Deliverables set out in Order Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Indemnifier"	a Party from whom an indemnity is sought under this Contract;
"Independent Control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of processing but does so separately from the Controller providing it with Personal Data and "**Independent Controller**" shall be construed accordingly;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Initial Period"	the initial term of a Contract specified on the Platform or the Order Form, as the context requires;
"Insolvency Event"	a) in respect of a person: b) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or c) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or d) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or f) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or h) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

	i) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or j) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;
"Intellectual Property Rights" or "IPR"	a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information; b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and c) all other rights having equivalent or similar effect in any country or jurisdiction;
"Invoicing Address"	the address to which the Supplier shall Invoice the Buyer as specified in the Order Form;
"IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies;
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of processing;
"Key Personnel"	the individuals (if any) identified as such in the Order Form;
"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	any Subcontractor: a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the

	aggregate Charges forecast to be payable under the Order Contract, and the Supplier shall list all such Key Subcontractors on the Platform and in the Key Subcontractor Section in the Order Form;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;
"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;
"Man Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks;
"Management Information"	the management information specified in DPS Schedule 5 (Management Levy and Information);
"Management Levy"	the sum specified on the Platform payable by the Supplier to CCS in accordance with DPS Schedule 5 (Management Levy and Information);
"Marketing Contact"	shall be the person identified in the DPS Appointment Form;
"MI Default"	means when two (2) MI Reports are not provided in any rolling six (6) month period;
"MI Failure"	means when an MI report: a) contains any material errors or material omissions or a missing mandatory field; or

	b) is submitted using an incorrect MI reporting Template; or c) is not submitted by the reporting date (including where a declaration of no business should have been filed);
"MI Report"	means a report containing Management Information submitted to the Authority in accordance with DPS Schedule 5 (Management Levy and Information);
"MI Reporting Template"	means the form of report set out in the Annex to DPS Schedule 5 (Management Levy and Information) setting out the information the Supplier is required to supply to the Authority;
"Milestone"	an event or task described as such in the Implementation Plan;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be achieved;
"Month"	a calendar month and "**Monthly**" shall be interpreted accordingly;
"National Insurance"	contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"New IPR"	a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; but shall not include the Supplier's Existing IPR;
"Occasion of Tax Non – Compliance"	where: a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of: i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related

	offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;
"Open Book Data"	complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Order Contract, including details and all assumptions relating to: a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables; b) operating expenditure relating to the provision of the Deliverables including an analysis showing: i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; ii) manpower resources broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each manpower grade; iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the DPS Contract Period and on an annual basis; f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and h) the actual Costs profile for each Service Period;
"Open Government Licence"	means the licensing terms for use of government intellectual property at: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/
"Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;

"Order Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the DPS Contract), which consists of the terms set out and referred to in the Order Form;
"Order Contract Period"	the Contract Period in respect of the Order Contract;
"Order Expiry Date"	the date of the end of an Order Contract as stated in the Order Form;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create an Order Contract;
"Order Form Template"	the template in DPS Schedule 6 (Order Form Template and Order Schedules);
"Order Incorporated Terms"	the contractual terms applicable to the Order Contract specified under the relevant heading in the Order Form;
"Order Initial Period"	the Initial Period of an Order Contract specified in the Order Form;
"Order Optional Extension Period"	such period or periods beyond which the Order Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form;
"Order Procedure"	the process for awarding an Order Contract pursuant to Clause 2 (How the contract works) and DPS Schedule 7 (Order Procedure);
"Order Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Order Contract;
"Order Start Date"	the date of start of an Order Contract as stated in the Order Form;
"Order Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following an Order Procedure and set out at Order Schedule 4 (Order Tender);
"Other Contracting Authority"	any actual or potential Buyer under the DPS Contract;

"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted by Law;
"Party"	in the context of the DPS Contract, CCS or the Supplier, and in the in the context of an Order Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits;
"Performance Indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the DPS Contract set out in DPS Schedule 4 (DPS Management);
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;
"Personnel"	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract;
"Platform"	the online application operated on behalf of CCS to facilitate the technical operation of the DPS;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies;
"Processing"	has the meaning given to it in the GDPR;
"Processor"	has the meaning given to it in the GDPR;
"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;

"Progress Report Frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
"Prohibited Acts"	a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or c) committing any offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;
"Protective Measures"	appropriate technical and organisational measures which may include pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in DPS Schedule 9 (Cyber Essentials), if applicable, in the case of the DPS Contract or Order Schedule 9 (Security), if applicable, in the case of an Order Contract;
"Recall"	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	the Supplier's plan (or revised plan) to rectify its breach using the template in Joint Schedule 10 (Rectification Plan Template)which shall include:

	a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
"Rectification Plan Process"	the process set out in Clause 10.4.3 to 10.4.5 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
"Reimbursable Expenses"	the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential Information"	a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR); b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and information derived from any of the above;
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;

"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
"Reminder Notice"	a notice sent in accordance with Clause 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Order Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For Information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
"Schedules"	any attachment to a DPS or Order Contract which contains important information specific to each aspect of buying and selling;
"Sectors and Domains"	the Sectors and Domains Filter Category defined in DPS Schedule 1;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Order Schedule 9 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Self Audit Certificate"	means the certificate in the form as set out in DPS Schedule 8 (Self Audit Certificate);
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Order Contract (which, where Order Schedule 14 (Service Credits) is used in this Contract, are specified in the Annex to Part A of such Schedule);
"Service Period"	has the meaning given to it in the Order Form;

"Services"	services made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Service Type"	means the Service Types Filter Category detailed in DPS Schedule 1
"Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;
"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
"Special Terms"	any additional Clauses set out in the DPS Appointment Form or Order Form which shall form part of the respective Contract;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in DPS Schedule 1 (Specification), as may, in relation to an Order Contract, be supplemented by the Order Form;
"Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in DPS Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;

	d) relevant Government codes of practice and guidance applicable from time to time;
"Start Date"	in the case of the DPS Contract, the date specified on the DPS Appointment Form, and in the case of an Order Contract, the date specified in the Order Form;
"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Order Procedure;
"Storage Media"	the part of any device that is capable of storing and retrieving data;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than an Order Contract or the DPS Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Supplier"	the person, firm or company identified in the DPS Appointment Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Order Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the DPS Appointment Form, or later defined in an Order Contract;
"Supplier's Confidential Information"	a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Order Contract and any alternative

	person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Order Contract;
"Supplier Non-Performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or c) comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of an Order Contract for the relevant period;
"Supplier Profit Margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"Supply Chain Information Report Template"	the document at Annex 1 of Joint Schedule 12 (Supply Chain Visibility);
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Order Contract detailed in the information are properly payable;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;
"Test"	any test required to be carried out pursuant to the Order Contract i) as set out in the Test Plan agreed pursuant to Part B of Order Schedule 13, ii) or as specified elsewhere in this Order Contract, and "Testing" and "Tested" shall be construed accordingly;
"Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;

"Transparency Information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and (ii) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Order Schedule 1 (Transparency Reports);
"US-EU Privacy Shield Register"	a list of companies maintained by the United States of America Department for Commence that have self-certified their commitment to adhere to the European legislation relating to the processing of personal data to non-EU countries which is available online at: https://www.privacyshield.gov/list;
"Variation"	has the meaning given to it in Clause 24 (Changing the contract);
"Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and
"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form.

Joint Schedule 2 (Variation Form)

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

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

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

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

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

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

Joint Schedule 3 (Insurance Requirements)

2. The insurance you need to have

2.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under an Order Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

2.1.1 the DPS Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

2.1.2 the Order Contract Effective Date in respect of the Additional Insurances.

2.2 The Insurances shall be:

2.2.1 maintained in accordance with Good Industry Practice;

2.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

2.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

2.2.4 maintained for at least six (6) years after the End Date.

2.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

3. How to manage the insurance

3.1 Without limiting the other provisions of this Contract, the Supplier shall:

3.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

3.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

3.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

4. What happens if you aren't insured

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

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

5. Evidence of insurance you must provide

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

6. Making sure you are insured to the required amount

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

7. Cancelled Insurance

7.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

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

8. Insurance claims

8.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

8.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 6.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

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

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

ANNEX: REQUIRED INSURANCES

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

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

1.2 public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than five million pounds (£5,000,000); and

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

Joint Schedule 4 (Commercially Sensitive Information)

2. What is the Commercially Sensitive Information?

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

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

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

No.	Date	Item(s)	Duration of Confidentiality
1.	29/04/2022	Supplier pricing	Order Form Contract Period

Order Schedule 4 (Order Tender)

[Redacted]

Social Value:

Supplier is expected to evidence how the Contract has had a positive impact on Social Value as outlined in B1 and B2 attached (Order Tender) during the Contract term.

Order Schedule 8 (Business Continuity and Disaster Recovery)

1. **BCDR PLAN**

1.1 At the Supplier's request, the Customer shall provide the Supplier with a copy of its Business Continuity & Disaster Recovery ("BCDR") Plan.

1.2 The Supplier shall develop a BCDR Plan and ensure that it is linked and integrated with the Buyer's BCDR Plan and the Supplier shall review and amend its BCDR Plan on a regular basis and as soon as is reasonably practicable on receipt of an amended Buyer BCDR Plan from the Buyer.

1.3 The Supplier shall ensure that its Sub-Contractor's BCDR Plans are integrated with the Supplier's BCDR Plan.

1.4 If there is a Disaster, the Parties shall, where applicable, implement their respective BCDR Plans and use all reasonable endeavours to re-establish their capacity to fully perform their obligations under this Order Contract. A Disaster will only relieve a Party of its obligations to the extent it constitutes a Force Majeure Event in accordance with Clause 20 (Circumstances Beyond Your Control).

Order Schedule 9 (Security)

Part B: Long Form Security Requirements

3. Definitions

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

"Breach of Security"	means the occurrence of: a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
"ISMS"	the information security management system and process developed by the Supplier in accordance with Paragraph 5 (ISMS) as updated from time to time in accordance with this Schedule; and
"Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

4. Security Requirements

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

4.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

4.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

4.3.1 **[Redacted]**

4.3.2 **[Redacted]**

4.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

4.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

4.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

4.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

4.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

5. Information Security Management System (ISMS)

5.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 5.4 to 5.6.

5.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

5.3 The Buyer acknowledges that;

5.3.1 If the Buyer has not stipulated during an Order Procedure that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

5.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

5.4 The ISMS shall:

5.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

5.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

5.4.3 at all times provide a level of security which:

(a) is in accordance with the Law and this Contract;

(b) complies with the Baseline Security Requirements;

(c) as a minimum demonstrates Good Industry Practice;

(d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

(e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)(https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

(f) takes account of guidance issued by the Centre for Protection of National Infrastructure https://www.cpni.gov.uk/

(g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

(h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

(i) addresses issues of incompatibility with the Supplier's own organisational security policies; and

(j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

5.4.4 document the security incident management processes and incident response plans;

5.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

5.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

5.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

5.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

5.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 5.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 5 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 5.4 to 5.6 shall be deemed to be reasonable.

5.8 Approval by the Buyer of the ISMS pursuant to Paragraph 5.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

6. Security Management Plan

6.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4.3 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 6.2.

6.2 The Security Management Plan shall:

6.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

6.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

6.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

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

6.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

6.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 5.4);

6.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

6.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

6.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

6.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

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

6.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 6.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-

submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 6.2 shall be deemed to be reasonable.

6.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 6.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

7. Amendment of the ISMS and Security Management Plan

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

7.1.1 emerging changes in Good Industry Practice;

7.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

7.1.3 any new perceived or changed security threats;

7.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;

7.1.5 any new perceived or changed security threats; and

7.1.6 any reasonable change in requirement requested by the Buyer.

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

7.2.1 suggested improvements to the effectiveness of the ISMS;

7.2.2 updates to the risk assessments;

7.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

7.2.4 suggested improvements in measuring the effectiveness of controls.

7.3 Subject to Paragraph 7.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 7.1, a Buyer request, a change to Annex nnex **1** (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

7.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster

than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

8. Security Testing

8.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

8.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

8.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

8.4 Where any Security Test carried out pursuant to Paragraphs 8.2 or 8.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

8.5 If any repeat Security Test carried out pursuant to Paragraph 8.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

9. Complying with the ISMS

9.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

9.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

9.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

10. Security Breach

10.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

10.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 10.1, the Supplier shall:

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

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

(b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

(c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the

Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

(d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

(e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

(f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

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

11. Vulnerabilities and fixing them

11.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

11.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

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

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

11.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

11.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the

Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

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

11.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

11.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

11.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

11.4.2 is agreed with the Buyer in writing.

11.5 The Supplier shall:

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

11.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

11.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

11.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 5.4.5;

11.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

11.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

11.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

11.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

11.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

11.7 A failure to comply with Paragraph 11.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

12. Handling Classified information

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

13. End user devices

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

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

14. Data Processing, Storage, Management and Destruction

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

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

14.3 The Supplier shall:

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

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

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

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

15. Ensuring secure communications

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

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

16. Security by design

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

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

17. Security of Supplier Staff

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

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

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

17.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information

management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

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

18. Restricting and monitoring access

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

19. Audit

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

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

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

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

19.3 The Supplier shall retain audit records collected in compliance with this Paragraph 19 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

‘Security Management Plan’ has been replaced with the completion of the ‘Information Security Questionnaire’ issued as part of the tender submission / prior to Contract Award.

Order Schedule 10 (Exit Management)

1. Within 20 (twenty) working days of the Start Date the Supplier must provide for the Buyer's Approval an exit plan which ensures continuity of service and which the Supplier will follow at the end of the Order Contract. The Buyer shall not unreasonably withhold Approval of the draft provided that the Supplier shall incorporate the Buyer's reasonable requirements in it
2. The Supplier must ensure that the exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its Replacement Supplier at the expiry or if the Order Contract ends before the scheduled expiry.
3. The exit plan should set out full details of timescales, activities and roles and responsibilities of the Parties for:
    - the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
    - the strategy for export and migration of Buyer data from any relevant Supplier system to the Buyer or a Replacement Supplier, including conversion to open standards or other standards required by the Buyer
    - the transfer of New IPR items to the Buyer or a Replacement Supplier
    - the testing and assurance strategy for exported Buyer data
    - if relevant, TUPE-related activity to comply with the TUPE regulations
    - any other activities and information which are reasonably required to ensure continuity of service during the exit period and an orderly transition to the Buyer or a Replacement Supplier.

Order Schedule 14 (Service Levels)

20. Definitions

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

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

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

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

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

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

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

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

21.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

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

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

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

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

22. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

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

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

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

Part A: Service Levels and Service Credits

23. Service Levels

If the level of performance of the Supplier:

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

23.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

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

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

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

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

24. Service Credits

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

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

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

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
To arrange and attend a scoping call / app demo	Response Times	2-business days or less	100%	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure
Routine testing & re-testing completed	Response Times	5-business days or less	100%	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure
Urgent testing completed	Response Times	2-business days or less	100%	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure

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

Formula: x% (Service Level Performance Measure) - x% (actual Service Level performance)	=	x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period)	=	11.5% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

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

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

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

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

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

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

3. Modern Slavery, Child Labour and Inhumane Treatment

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

3.1 The Supplier:

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

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

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

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

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

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

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

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

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

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

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

4. Income Security

4.1 The Supplier shall:

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

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

4.1.3 ensure that all workers are provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

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

5. Working Hours

5.1 The Supplier shall:

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

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

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

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

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

5.3.1 this is allowed by national law;

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

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

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

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

6. Sustainability

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

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

Appendix 1 – Security Requirements Level 1 and 2

(Schedule 6 of the Framework)

MINIMUM SECURITY REQUIREMENTS

GENERAL

The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Appendix 1 to the Contract (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Contractor's Systems Environment.

Terms used in this Appendix 1 which are not defined below shall have the meanings given to them in Joint Schedule 1 (Definitions and Interpretation) of the Contract.

1. DEFINITIONS

1.1 In this Appendix 1, the following definitions shall apply:

"Authority Personnel"	shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, contractors and suppliers but excluding the Contractor and any Sub-contractor (as applicable).
"**Cyber Essentials**"	shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Good Security Practice**"	shall mean: a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for

Standardization or the National Institute of Standards and Technology);

b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and

the Government's security policies, frameworks, standards and guidelines relating to Information Security.

"**Information Security**" shall mean:

a) the protection and preservation of:

i) the confidentiality, integrity and availability of any Authority Assets, the Authority's Systems Environment (or any part thereof) and the Contractor's Systems Environment (or any part thereof);
ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and

b) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.

"**Information Security Manager**" shall mean the person appointed by the Contractor with the appropriate experience, authority and expertise to ensure that the Contractor complies with the Authority's Security Requirements.

"**Information Security Management System ("ISMS")**" shall mean the set of policies, processes and systems designed, implemented and maintained by the Contractor to manage Information Security Risk as specified by ISO/IEC 27001.

"**Information Security Questionnaire**" shall mean the Authority's set of questions used to audit and on an ongoing basis assure the

	Contractor's compliance with the Authority's Security Requirements. c)
"**Information Security Risk**"	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.
"**ISO/IEC 27001, ISO/IEC 27002 and ISO 22301**	shall mean a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301 in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO.
"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable).
"**Risk Profile**"	shall mean a description of any set of risk. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.

1.2 Reference to any notice to be provided by the Contractor to the Authority shall be construed as a notice to be provided by the Contractor to the Authority's Representative.

2. PRINCIPLES OF SECURITY

2.1 The Contractor shall at all times comply with the Authority's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE AND AUDIT

3.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with ISO/IEC 27001.

3.2 The Contractor shall appoint an Information Security Manager and shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.

3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract Period and that the Information Security Management System meets Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Contract);
b) a risk assessment (which shall include any risks specific to the Services);
c) a statement of applicability;
d) a risk treatment plan; and
e) an incident management plan
in each case as specified by ISO/IEC 27001.

The Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

3.4 The Contractor shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Authority.

3.5 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Authority may, in its absolute discretion, notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Contractor shall, at its own expense, undertake those actions required in order to comply with the Authority's Security Requirements within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Authority's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause 10.4.1.

4. CYBER ESSENTIALS SCHEME

4.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials (the "Cyber Essentials Certificate") in relation to the Services during Contract Period. The Cyber Essentials Certificate shall be provided by the Contractor to the Authority annually on the dates as agreed by the Parties.

4.2 The Contractor shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Contractor shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the Contract Period after the first date on which the Contractor was required to provide a Cyber Essentials Certificate in accordance with paragraph **Error!**

Reference source not found. (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause 10.4.1.

5. RISK MANAGEMENT

5.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority's own risk management processes regarding the Services.

5.2 For the avoidance of doubt, the Contractor shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph **Error! Reference source not found.**. Any failure by the Contractor to comply with any requirement of this paragraph **Error! Reference source not found.** (regardless of whether such failure is capable of remedy), shall constitute a Material Breach entitling the Authority to exercise its rights under clause 10.4.1.

6. SECURITY AUDIT AND ASSURANCE

6.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Authority (the "**Information Security Questionnaire**") at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

6.2 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Contractor's Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Contractor shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Contractor shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.

6.3 The Authority shall schedule regular security governance review meetings which the Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

7. SECURITY POLICIES AND STANDARDS

7.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A.

7.2 Notwithstanding the foregoing, the Authority's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change

constitutes a Contract Change, any change in the Authority's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any change in the Authority's Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

7.3 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Physical Security Policy

d) Information Management Policy

e) Email Policy

f) Remote Working Policy

g) Social Media Policy

h) Security Classification Policy

i) HMG Personnel Security Controls – May 2018
(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)