

DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE: C2937

THE BUYER: Intellectual Property Office

BUYER ADDRESS REDACTED

THE SUPPLIER: Cyberis Limited

SUPPLIER ADDRESS: REDACTED

REGISTRATION NUMBER: 07556994

DUNS NUMBER: 21-716-9431

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 1 August 2023. 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, CHECK, Clearance: Security Check (SC), Networks, Database, Cloud, Endpoint/applications, 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 7 (Financial Difficulties)

Crown Copyright 2020

- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

- Order Schedules for RM3764iii

- Order Schedule 4 (Order Tender)
- Order Schedule 5 (Pricing Details)
- Order Schedule 6 (ICT Services)
- Order Schedule 7 (Key Supplier Staff)
- Order Schedule 8 (Business Continuity and Disaster Recovery)
- Order Schedule 9 (Security)
- Order Schedule 10 (Exit Management)
- Order Schedule 15 (Order Contract Management)
- Order Schedule 18 (Background Checks)
- Order Schedule 20 (Order Specification)
- Order Schedule 22 (Secret Matters)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6
7. Order Schedule 4 (Order Tender) as long as any parts of the Order Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

The following Special Terms are incorporated into this Order Contract:

Non-Disclosure Agreement as signed by Cyberis Limited

ORDER START DATE: 17 August 2023

ORDER EXPIRY DATE: 14 August 2026

ORDER INITIAL PERIOD: 3 Years

ORDER OPTIONAL EXTENSION: None

DPS Ref: RM3764iii

Model Version: v1.0

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

DELIVERABLES

See details in Order Schedule 20 (Order Specification)

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:
£164,160.00

ORDER CHARGES

See details in Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES

Recoverable as stated in the DPS Contract

PAYMENT METHOD

Payment method(s) and necessary details to be advised at award

BUYER'S INVOICE ADDRESS:

Payment will only be made on satisfactory delivery of the agreed Penetration Testing services. Before payment, any invoices that are received must include a detailed breakdown of the work completed, the associated costs and a quote reference number. All invoices must quote a relevant IPO Purchase Order and Contract reference number and be emailed to REDACTED

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED

BUYER'S ENVIRONMENTAL POLICY

[Our energy use - Intellectual Property Office - GOV.UK \(www.gov.uk\)](#)

BUYER'S SECURITY POLICY

[Security Policy for Contractors.pdf](#)

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED

DPS Ref: RM3764iii

Model Version: v1.0

SUPPLIER'S CONTRACT MANAGER

REDACTED

PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY

Quarterly on the first Working Day of each quarter

KEY STAFF

N/A

KEY SUBCONTRACTOR(S)

None used

COMMERCIALLY SENSITIVE INFORMATION

N/A

SERVICE CREDITS

Not applicable

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) and as in the statement submitted by Cyberis Limited in response to Question 2.7 of the Key Participation Requirements within Appendix C – Response Guidance.

Signed by an authorised signatory for and behalf of the Supplier

Supplier_Signature

REDACTED

REDACTED

16 August 2023

For and on behalf of the Buyer

Contracting_Authority_Signature

REDACTED

REDACTED

16 August 2023

Joint Schedules for RM3764iii

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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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"	<p>the Relevant Authority's right to:</p> <ul style="list-style-type: none"> 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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	<p>b) the Relevant Authority's statutory or regulatory auditors;</p> <p>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;</p> <p>d) HM Treasury or the Cabinet Office;</p> <p>e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and</p> <p>f) successors or assigns of any of the above;</p>
"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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"Central Government Body"	<p>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:</p> <p>a) Government Department;</p> <p>b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);</p> <p>c) Non-Ministerial Department; or</p> <p>d) Executive Agency;</p>
"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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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

DPS Ref: RM3764iii

Model Version: v1.0

	<p>not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;</p> <p>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;</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;</p> <p>but excluding:</p> <p>a) Overhead;</p> <p>b) financing or similar costs;</p> <p>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;</p> <p>d) taxation;</p> <p>e) fines and penalties;</p> <p>f) non-cash items (including depreciation, amortisation, impairments and movements in provisions);</p>
"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"	<p>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:</p> <p>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;</p> <p>b) is required by the Supplier in order to provide the Deliverables; and/or</p> <p>c) has been or shall be generated for the purpose of providing the Deliverables;</p>
"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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	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"	<p>any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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),

DPS Ref: RM3764iii

Model Version: v1.0

	as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <ul style="list-style-type: none"> 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"	<ul style="list-style-type: none"> 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

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	<p>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</p> <p>e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or</p> <p>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</p> <p>g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or</p> <p>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</p> <p>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</p> <p>j) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;</p>
"Intellectual Property Rights" or "IPR"	<p>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;</p> <p>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</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction;</p>
"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

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	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"	<p>any Subcontractor:</p> <ul style="list-style-type: none"> 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, <p>and the Supplier shall list all such Key Subcontractors on the Platform and in the Key Subcontractor Section in the Order Form;</p>
"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

DPS Ref: RM3764iii

Model Version: v1.0

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	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: <ul style="list-style-type: none"> 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"	<ul style="list-style-type: none"> 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; <p>but shall not include the Supplier's Existing IPR;</p>

"Occasion of Tax Non – Compliance"	<p>where:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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"	<p>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:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	<p>e) the Supplier Profit achieved over the DPS Contract Period and on an annual basis;</p> <p>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;</p> <p>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</p> <p>h) the actual Costs profile for each Service Period;</p>
"Open Government Licence"	<p>means the licensing terms for use of government intellectual property at:</p> <p>http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/</p>
"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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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"	<p>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:</p> <ul style="list-style-type: none">i) induce that person to perform improperly a relevant function or activity; orii) reward that person for improper performance of a relevant function or activity; <p>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</p> <p>c) committing any offence:</p> <ul style="list-style-type: none">i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); orii) under legislation or common law concerning fraudulent acts; oriii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or <p>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;</p>
"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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	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);

DPS Ref: RM3764iii

Model Version: v1.0

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	<p>c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;</p> <p>d) relevant Government codes of practice and guidance applicable from time to time;</p>
"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"	<p>any contract or agreement (or proposed contract or agreement), other than an Order Contract or the DPS Contract, pursuant to which a third party:</p> <p>a) provides the Deliverables (or any part of them);</p> <p>b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or</p> <p>c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);</p>
"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"	<p>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;</p> <p>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;</p> <p>c) Information derived from any of (a) and (b) above;</p>

"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;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

"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 Commerce 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)

DPS Ref: RM3764iii

Model Version: v1.0

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

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: <ul style="list-style-type: none"> [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)

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

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
	N/A	N/A	N/A

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>

Cyberis Limited response to Key Participation Requirements (Question 2.7) with regard to Theme 5: Wellbeing, outlining their current approach to the following:

- Demonstrating action to support the health and wellbeing, including physical and mental health, in the contract workforce
- Influencing staff, suppliers, customers and communities through the delivery of the contract to support health and wellbeing, including physical and mental health.

Cyberis is a growing SME with a fully remote working workforce. The health and wellbeing of our colleagues is important to us, and we strive to create an inclusive and supportive environment for all employees. We have proactively taken steps to improve the health and wellbeing of our colleagues (for example, dynamically varying working patterns to support out colleagues' changing personal needs, helping to combat the stress of social isolation with virtual social events and accommodating requests for role and responsibility changes to accommodate changing mental health needs) and offered support and flexibility to our limited number of suppliers, particularly through the COVID-19 pandemic.

Furthermore, Cyberis organises biannual team social events to support team building and wellbeing throughout the company by fostering a community spirit. As a

small business, the health and wellbeing of our colleagues and a positive working environment are particularly important to us.

As we grow, we recognise the need to do more to support wellbeing. We have recently re-structured the business to appoint additional line managers to allow capacity for effective people management and regular one to one time with colleagues, which is particularly important for our remote workers. We will shortly be launching a comprehensive Employee Assistance Programme, open to all employees, which will provide free and confidential advice and support for wellbeing issues, including mental health issues and financial problems causing stress and anxiety. As a member of Cyber Scheme, we volunteer ten consultant-days per year to support community projects coordinated by the Cyber Scheme. We support IASME's neurodiverse cyber security training programme by volunteering time to provide careers talks to attendees.

Joint Schedule 6 (Key Subcontractors)

3. Restrictions on certain subcontractors

- 3.1 The Supplier is entitled to sub-contract its obligations under the DPS Contract to the Key Subcontractors identified on the Platform.
- 3.2 The Supplier is entitled to sub-contract its obligations under an Order Contract to Key Subcontractors listed on the Platform who are specifically nominated in the Order Form.
- 3.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 3.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a New Key Subcontractor then they will be added to the Platform. Where the Buyer consents to the appointment of a New Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
 - 3.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 3.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 3.3.3 the proposed Key Subcontractor employs unfit persons.
- 3.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - 3.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

- 3.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
- 3.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;
- 3.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected DPS Price over the DPS Contract Period;
- 3.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Order Contract Period; and
- 3.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 3.4, the Supplier shall also provide:
 - 3.5.1 a copy of the proposed Key Sub-Contract; and
 - 3.5.2 any further information reasonably requested by CCS and/or the Buyer.
- 3.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
 - 3.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;
 - 3.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
 - 3.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
 - 3.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
 - 3.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the DPS Contract in respect of:
 - (a) the data protection requirements set out in Clause 14 (Data protection);
 - (b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);
 - (c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
 - (d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
 - (e) the conduct of audits set out in Clause 6 (Record keeping and reporting);

- 3.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
- 3.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 7 (Financial Difficulties)

4. Definitions

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

"Credit Rating Threshold"	the minimum credit rating level for the Monitored Company as set out in the third Column of the table at Annex 2 and
"Financial Distress Event"	<p>the occurrence or one or more of the following events:</p> <ul style="list-style-type: none">a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold;b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party;d) Monitored Company committing a material breach of covenant to its lenders;e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or

- f) any of the following:
 - i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;
 - ii) non-payment by the Monitored Company of any financial indebtedness;
 - iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or
 - iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company

in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Order Contract;

"Financial Distress Service Continuity Plan"

a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with each Order Contract in the event that a Financial Distress Event occurs;

"Monitored Company"

Supplier [the DPS Guarantor/ [and Order Guarantor] or any Key Subcontractor]

"Rating Agency"

the rating agency stated in Annex 1.

5. When this Schedule applies

- 5.1 The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.
- 5.2 The terms of this Schedule shall survive termination or expiry of this Contract.

6. What happens when your credit rating changes

- 6.1 The Supplier warrants and represents to CCS that as at the Start Date the credit rating issued for the Monitored Companies by the Rating Agency is as set out in Annex 2.
- 6.2 The Supplier shall promptly (and in any event within ten (10) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by

the Rating Agency for a Monitored Company which means that the credit rating for the Monitored company falls below the Credit Rating Threshold.

- 6.3 If there is any such downgrade credit rating issued by the Rating Agency for a Monitored Company the Supplier shall at CCS' request ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

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

where:

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

- 6.4 The Supplier shall:

6.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agency; and

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

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

7. What happens if there is a financial distress event

- 7.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 7.3 to 7.6.
- 7.2 In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:
 - 7.2.1 rectify such late or non-payment; or
 - 7.2.2 demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.
- 7.3 The Supplier shall and shall procure that the other Monitored Companies shall:
 - 7.3.1 at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and
 - 7.3.2 where CCS reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:
 - (a) submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and
 - (b) provide such financial information relating to the Monitored Company as CCS may reasonably require.
- 7.4 If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.
- 7.5 If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete

or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

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

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

7.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 7.5 and 7.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

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

7.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 7.6.

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

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

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

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

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

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

9. What happens If your credit rating is still good

9.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agency reviews and reports

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

subsequently that the credit rating does not drop below the relevant Credit Rating Threshold, then:

- 9.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and
- 9.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

ANNEX 1: RATING AGENCY

Dun & Bradstreet

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (D&B Failure Rating)	Credit Rating Threshold
Supplier	[D&B Failure Rating]	[D&B Failure Rating – 10%]
[DPS Guarantor/ [and Order Guarantor]	[D&B Failure Rating]	[D&B Failure Rating – 10%]
[Key Subcontractor]	[D&B Failure Rating]	[D&B Failure Rating – 10%]

Joint Schedule 10 (Rectification Plan)

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

Reasons for Rejection (if applicable)	[add reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Status of the Controller

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:
 - (a) “Controller” in respect of the other Party who is “Processor”;
 - (b) “Processor” in respect of the other Party who is “Controller”;
 - (c) “Joint Controller” with the other Party;
 - (d) “Independent Controller” of the Personal Data where there other Party is also “Controller”,

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

Where one Party is Controller and the other Party its Processor

2. Where a Party is a Processor, the only processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller.
3. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Services;

- (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
 - (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

- (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
 - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Request (or purported Data Subject Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Data Loss Event.
7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller in phases, as details become available.
8. Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Data Loss Event; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
12. Before allowing any Sub-processor to Process any Personal Data related to the Contract, the Processor must:
- (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
 - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
14. The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable

controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

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

Where the Parties are Joint Controllers of Personal Data

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

Independent Controllers of Personal Data

17. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
18. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
21. The Parties shall only provide Personal Data to each other:
 - (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
22. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each

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

23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.
24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
 - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
 - (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

- (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
- 27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
- 28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data A) Template

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

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: REDACTED
- 1.2 The contact details of the Supplier's Data Protection Officer are: REDACTED
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none">• With the exception of Cyberis Limited employee data, all other personal data handled under the contract will be controlled by IPO and Cyberis Limited will rely on instructions from IPO in terms of how to handle such data should it be encountered in the course of delivery of tests under this contract.
Duration of the Processing	<p>Throughout the duration of the contract. The Supplier may retain Personal Data that it has processed pursuant to the Call-Off Contract upon termination or expiry of the Call-Off Contract for whatever reason for a period of seven years or such longer period as is required in order to comply with professional and regulatory requirements. If required by law to retain a copy, the Supplier shall inform the Buyer what it is retaining and the legal reason why it needs to be retained.</p>
Nature and purposes of the Processing	<p>The Parties will Process Personal Data in the context of:</p> <ul style="list-style-type: none">• requests for services and the provision of all aspects of CHECK approved Penetration Testing as outlined in the specification (Order Schedule 20).• management of the Call-Off Contract and associated activities

	The Buyer and Supplier will carry out processing for the purposes of enabling completion of the Services as described in Call-Off Schedule 20 (Call-Off Specification).
Type of Personal Data	IPO (Buyer) Staff & Supplier Staff names, email addresses, identification number, IP addresses, telephone numbers, IP data location data of staff and such other Personal Data as is required to meet the objectives/specification of the Call-Off Contract.
Categories of Data Subject	The Data Subjects will include: <ul style="list-style-type: none"> • Individuals working for the Buyer; • Individuals working for the Supplier; • Individuals with whom the Buyer does business (whether directly or through their employer) or otherwise has dealings with.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	According to IPO disposal & retention policies (or as otherwise agreed by the Parties in writing)

B) DPS Contract Personal Data Processing

Description	Details
Identity of Controller for each Category of Personal Data	<p>CCS is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 and for the purposes of the Data Protection Legislation, CCS is the Controller and the Supplier is the Processor of the Personal Data recorded below</p>
Duration of the Processing	Up to 7 years after the expiry or termination of the DPS Contract
Nature and purposes of the Processing	<p>To facilitate the fulfilment of the Supplier's obligations arising under this DPS Contract including</p> <ul style="list-style-type: none"> i. Ensuring effective communication between the Supplier and CSS ii. Maintaining full and accurate records of every Order Contract arising under the Framework Agreement in accordance with Core Terms Clause 15 (Record Keeping and Reporting)
Type of Personal Data	<p>Includes:</p> <ul style="list-style-type: none"> i. Contact details of, and communications with, CSS staff concerned with management of the DPS Contract ii. Contact details of, and communications with, Buyer staff concerned with award and management of Order Contracts awarded under the DPS Contract, iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract <p>Contact details, and communications with Supplier staff concerned with management of the DPS Contract</p>
Categories of Data Subject	<p>Includes:</p> <ul style="list-style-type: none"> i. CSS staff concerned with management of the DPS Contract ii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the DPS Contract

	<p>iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract</p> <p>Supplier staff concerned with fulfilment of the Supplier's obligations arising under this DPS Contract</p>
<p>Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p>All relevant data to be deleted 7 years after the expiry or termination of this DPS Contract unless longer retention is required by Law or the terms of any Order Contract arising hereunder</p>

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Law in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Law as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

- (a) report to the other Party every [x] months on:
 - (i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);
 - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
 - (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

- (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
 - (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,
- that it has received in relation to the subject matter of the Contract during that period;
- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject before disclosing or transferring the Personal Data to the third party. For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their duties under this Annex 2 (Data Sharing Agreement) and those in respect of Confidential Information
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Law;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

- (i) nature of the data to be protected;
 - (i) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Law, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
- (i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Law and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Law to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;
- (b) all reasonable assistance, including:
 - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
 - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
 - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach;
- and
- (f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Law; and/or
- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

- (a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute

shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“**Court**”) by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “**Claim Losses**”):

- (a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
- (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Control Memorandum of Understanding*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 (*Ending the contract*).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Law.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Law and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Law and its privacy policy.

Order Schedules for RM3764iii

Order Schedule 4 (Order Tender)

REDACTED

Order Schedule 5 (Pricing Details)

REDACTED

For the avoidance of doubt, the total contract value will not exceed £427,680.00 exc. VAT. These rates are to remain firm for the duration of the contract.

Order Schedule 6 (ICT Services)

1. Definitions

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

0.1 **"Buyer
Software"**

0.2 any software which is owned by or
licensed to the Buyer and which is or will be
used by the Supplier for the purposes of
providing the Deliverables;

0.3	"Buyer System"	0.4	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Order Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
0.5	"Commercial off the shelf Software" or "COTS Software"		non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms;
0.6	"Defect"		any of the following: a) any error, damage or defect in the manufacturing of a Deliverable; or b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or
0.7			c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract; or d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract;
0.8	"ICT Environment"	0.9	the Buyer System and the Supplier System;
0.10	"Licensed Software"	0.11	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or

		pursuant to this Order Contract, including any COTS Software;
0.12	"New Release"	0.13 an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
0.14	"Open Source Software"	0.15 computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
0.16	"Operating Environment"	0.17 means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: <ul style="list-style-type: none"> e) the Deliverables are (or are to be) provided; or f) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or g) where any part of the Supplier System is situated;
0.18	"Quality Plans"	0.19 has the meaning given to it in paragraph 6.1 of this Schedule;
0.20	"Sites"	0.21 has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Order Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
0.22	"Software"	0.23 Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
0.24	"Software Supporting Materials"	0.25 has the meaning given to it in paragraph 8.1 of this Schedule;

0.26 "Source Code"	0.27	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
0.28 "Specially Written Software"	0.29	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
0.30 "Supplier System"	0.31	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

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

3. Buyer due diligence requirements

- 3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
- 3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
 - 3.1.2. operating processes and procedures and the working methods of the Buyer;
 - 3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
 - 3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to

or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

- 3.2. The Supplier confirms that it has advised the Buyer in writing of:
 - 3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the Deliverables;
 - 3.2.2. the actions needed to remedy each such unsuitable aspect; and
 - 3.2.3. a timetable for and the costs of those actions.

4. Software warranty

- 4.1. The Supplier represents and warrants that:
 - 4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Order Contract including the receipt of the Deliverables by the Buyer;
 - 4.1.2. all components of the Specially Written Software shall:
 - 4.1.2.1. be free from material design and programming errors;
 - 4.1.2.2. perform in all material respects in accordance with the relevant specifications and Documentation; and
 - 4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

- 5.1. The Supplier shall:
 - 5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with any interface requirements of the Buyer specified in this Order Contract and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;
 - 5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
 - 5.1.3. ensure that the Supplier System will be free of all encumbrances;
 - 5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Order Contract;
 - 5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

- 6.1. The Supplier shall, where specified by the Buyer as part of their Order Procedure, and in accordance with agreed timescales, develop quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").
- 6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.
- 6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
- 6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Order Contract Period:
 - 6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Order Contract;
 - 6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
 - 6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

- 7.1. The Supplier shall allow any auditor access to the Supplier premises to:
 - 7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);
 - 7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
 - 7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Intellectual Property Rights in ICT

8.1. Assignments granted by the Supplier: Specially Written Software

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

- 8.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
 - 8.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").
- 8.1.2. The Supplier shall:
 - 8.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
 - 8.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and
 - 8.1.2.3. without prejudice to paragraph 8.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.
- 8.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.
- 8.2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**
 - 8.2.1. Unless the Buyer gives its Approval the Supplier must not use any:
 - a) of its own Existing IPR that is not COTS Software;
 - b) third party software that is not COTS Software
 - 8.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a

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

8.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 8.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

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

8.2.3.2. only use such third party IPR as referred to at paragraph 8.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

8.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 8.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

8.2.5. The Supplier may terminate a licence granted under paragraph 8.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

8.3. Licenses for COTS Software by the Supplier and third parties to the Buyer

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

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

8.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 8.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

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

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

8.3.4.2. will no longer be made commercially available

8.4. Buyer's right to assign/novate licences

8.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 8.2 (to:

8.4.1.1. a Central Government Body; or

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

8.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 8.2.

8.5. Licence granted by the Buyer

8.5.1. The Buyer grants to the Supplier a licence to use the Specially Written Software i) during the Order Contract Period for the purpose of fulfilling its obligations under the Order Contract, and ii) after the Contract period on the terms set out in the Open Government Licence.

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

8.6. Open Source Publication

8.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 8.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

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

- 8.6.1.2. based on Open Standards (where applicable),
- 0.31.1 and the Buyer may, at its sole discretion, publish the same as Open Source.
- 8.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:
 - 8.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;
 - 8.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
 - 8.6.2.3. do not contain any material which would bring the Buyer into disrepute;
 - 8.6.2.4. can be published as Open Source without breaching the rights of any third party;
 - 8.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and
 - 8.6.2.6. do not contain any Malicious Software.
- 8.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:
 - 8.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
 - 8.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9. Supplier-Furnished Terms

9.1. Software Licence Terms

- 9.1.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 8.2.3 are detailed in Annex A of this Order Schedule 6.
- 9.1.1.2. Terms for licensing of COTS software in accordance with Paragraph 8.3 are detailed in Annex B of this Order Schedule 6.

ANNEX A

Non-COTS Third Party Software Licensing Terms

ANNEX B
COTS Licensing Terms

Order Schedule 7 (Key Supplier Staff)

- 0.32 1. The Annex 1 to this Schedule lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
- 0.33
- 0.34 2. The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 0.35
- 0.36 3. The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 0.37
- 0.38 4. The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
- 0.39
- 0.39.1 4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
- 0.39.2 4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
- 0.39.3 4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
- 0.39.4
- 0.40 5. The Supplier shall:
- 0.40.1 5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
- 0.40.2 5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
- 0.40.3 5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least [] Months’ notice;
- 0.40.4 5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

0.40.5 5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

0.40.6

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

Annex 1- Key Roles

Key Role	Key Staff	Contact Details

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)

1. Part B: Long Form Security Requirements

2. Definitions

- 2.1 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: <ul style="list-style-type: none">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/orb) 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 4 (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.

3. Security Requirements

- 3.1 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.

- 3.2 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.
- 3.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:
 - 3.3.1 [insert security representative of the Buyer – To be advised at award]
 - 3.3.2 [insert security representative of the Supplier – to be advised at award]
- 3.4 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.
- 3.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.
- 3.6 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.
- 3.7 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.
- 3.8 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.

4. Information Security Management System (ISMS)

- 4.1 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 4.4 to 4.6.
- 4.2 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.
- 4.3 The Buyer acknowledges that;
 - 4.3.1 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

4.3.2 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.

4.4 The ISMS shall:

4.4.1 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;

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

4.4.3 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;

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

- 4.4.5 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
- 4.4.6 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).
- 4.5 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.
- 4.6 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.
- 4.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 4.1 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 4 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 4.4 to 4.6 shall be deemed to be reasonable.
- 4.8 Approval by the Buyer of the ISMS pursuant to Paragraph 4.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

5. Security Management Plan

- 5.1 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 5.2.

5.2 The Security Management Plan shall:

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

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

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

5.2.4 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;

5.2.5 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;

5.2.6 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 4.4);

5.2.7 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);

5.2.8 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;

- 5.2.9 set out the scope of the Buyer System that is under the control of the Supplier;
 - 5.2.10 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
 - 5.2.11 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.
- 5.3 If the Security Management Plan 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 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 5.2 shall be deemed to be reasonable.
- 5.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 5.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

6. Amendment of the ISMS and Security Management Plan

- 6.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:
- 6.1.1 emerging changes in Good Industry Practice;
 - 6.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
 - 6.1.3 any new perceived or changed security threats;
 - 6.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
 - 6.1.5 any new perceived or changed security threats; and
 - 6.1.6 any reasonable change in requirement requested by the Buyer.

- 6.2 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:
- 6.2.1 suggested improvements to the effectiveness of the ISMS;
 - 6.2.2 updates to the risk assessments;
 - 6.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
 - 6.2.4 suggested improvements in measuring the effectiveness of controls.
- 6.3 Subject to Paragraph 6.4, 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 6.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
- 6.4 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.

7. Security Testing

- 7.1 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.
- 7.2 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.
- 7.3 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.

- 7.4 Where any Security Test carried out pursuant to Paragraphs 7.2 or 7.3 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.
- 7.5 If any repeat Security Test carried out pursuant to Paragraph 7.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

8. Complying with the ISMS

- 8.1 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.
- 8.2 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.
- 8.3 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.

9. Security Breach

- 9.1 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.
- 9.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 9.1, the Supplier shall:
- 9.2.1 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.
- 9.3 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.

10. Vulnerabilities and fixing them

- 10.1 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.
- 10.2 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:
 - 10.2.1 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
 - 10.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.
- 10.3 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:
 - 10.3.1 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;
 - 10.3.2 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
 - 10.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.
- 10.4 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:

- 10.4.1 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
- 10.4.2 is agreed with the Buyer in writing.
- 10.5 The Supplier shall:
 - 10.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;
 - 10.5.2 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;
 - 10.5.3 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;
 - 10.5.4 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 4.4.5;
 - 10.5.5 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;
 - 10.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;
 - 10.5.7 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
 - 10.5.8 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.
- 10.6 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.

- 10.7 A failure to comply with Paragraph 10.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

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

2. End user devices

- 2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").
- 2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the 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.

3. Data Processing, Storage, Management and Destruction

- 3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.
- 3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

- 3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;
- 3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
- 3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

- 4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA.
- 4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

- 5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
- 5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (<https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

- 6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
- 6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

- 6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
- 6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
- 6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

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

8. Audit

- 8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:
 - 8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
 - 8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
- 8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

[]

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 15 (Order Contract Management)

1. Definitions

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

"Operational Board" the board established in accordance with paragraph 5.1 of this Schedule;

"Project Manager" the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

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

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

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

3. Role of the Supplier Contract Manager

- 3.1 The Supplier's Contract Manager shall be:

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

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

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

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

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

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

4. Contract Risk Management

- 4.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Order Contract.
- 4.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
 - 4.2.1 **the identification and management of risks;**
 - 4.2.2 the identification and management of issues; and
 - 4.2.3 monitoring and controlling project plans.
- 4.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 4.4 The Supplier will maintain a risk register of the risks relating to the Order Contract which the Buyer and the Supplier have identified.

5. ROLE OF THE OPERATIONAL BOARD

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

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

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

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

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

Annex: Contract Boards

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

Guidance note: Details of additional boards to be inserted.

Order Schedule 18 (Background Checks)

9. When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on the Contract.

10. Definitions

“Relevant Conviction” means any conviction listed in Annex 1 to this Schedule.

11. Relevant Convictions

11.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

11.2 Notwithstanding Paragraph 3.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

- (a) carry out a check with the records held by the Department for Education (DfE);
- (b) conduct thorough questioning regarding any Relevant Convictions; and
- (c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

All that are relevant to this contract

Order Schedule 20 (Order Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Order Contract

1. SUMMARY

- 1.1** It is a UK Government and NCSC mandatory requirement that that a full annual Network Penetration Test is carried out by a CHECK approved Penetration Testing company. In addition to this any new IT services developed are also Penetration Tested prior to go live date.
- 1.2** Penetration Tests will be required for:
- on-premises and mobile infrastructure consisting of networking, virtualised servers and appliances, active directory, firewall rules and end user devices
 - cloud architecture consisting primarily of serverless architecture, storage, databases, and networking components
 - web applications and API's
 - internal and external testing required
- 1.3** Reports to be produced and distributed to IPO securely and marked as "Official – Sensitive" in an easily consumable format from which findings can be exported into other formats for management.

2. BACKGROUND TO THE IPO

- 2.1** The Intellectual Property Office (IPO) - an operating name of the Patent Office - is an Executive Agency of the Department for Science, Innovation and Technology (DSIT). It aims to stimulate innovation and enhance the international competitiveness of British industry and commerce. It offers customers an accessible, high quality, value for money system both nationally and internationally, for granting intellectual property rights.
- 2.2** The IPO is a highly successful organisation which, over its 155-year history, has adapted its approach and services to meet changing demands. Its core business and products deliver high quality, cost effective Intellectual Property (IP) rights to customers and its success in these core areas is tied to a much wider range of activities, such as awareness-raising and enforcement. Its customers operate within both the UK and global economies. Further information about the IPO can be found on its website at: www.ipo.gov.uk
- 2.3** The number of people currently employed by the IPO is approximately REDACTED It is based at three sites: REDACTED . It is primarily located at the Newport site.
- 2.4** IPO Secure is the department within deals with all aspects of security within the IPO. Our work is vital to the success and reputation of the IPO. Keeping

information safe and secure ensures the information required by IPO staff to undertake their roles is available when required.

3. BACKGROUND TO THE REQUIREMENT

3.1 Penetration testing is required to validate the security of IPO's systems, applications, and networks. IPO Secure need a Potential Provider for ongoing support for penetration testing in order to perform routine scheduled testing throughout the year, and also to perform ad-hoc tests of systems when new services are developed or significantly changed.

3.2 The IPO has a hybrid workforce using mobile Windows based devices. It has existing systems and services that serve the needs both of customers for applying for and managing their Intellectual Property rights, and for internal users for examining, managing, and publishing those rights largely running as web applications on a traditional server-based architecture. IPO also has a significant transformation programme underway to develop new rights granting systems in a serverless cloud architecture.

Approximate scale of infrastructure detailed below:

End User devices	Number
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
On-premises devices	Number
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
Cloud Architecture	
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED

3.3 Historically, the IPO undertook an annual penetration test / health check of its entire estate, delivered by an independent third-party security assurance company, under the terms and conditions of the NCSC CHECK scheme, as mandated by NCSC.

3.4 This approach to penetration testing of the estate proved to be ineffective at enabling IPO to reduce the risk inherent in its systems and did not provide an ongoing up-to-date picture of the state of vulnerability and risk across the estate.

The reasons for this were identified as follows:

- Penetration testing was conducted annually with a 12-month gap
- Vulnerabilities are reported back to IPO in one unmanageable 'super report.'
- The quantity of reported vulnerabilities was significant, presenting difficulties in prioritisation of effort.
- 12-month gaps between 'audits' reduced urgency in remediation of risks, leading to inaction and extended window of opportunity for compromise.

3.5 Subsequently the IPO moved to a model where several scopes were defined to allow a six monthly cycle of testing and retesting of more manageable portions of the estate which has helped with the above problems. This, or a similar approach, is required for this contract.

4. DEFINITIONS

Expression/Acronym	Definition
API's	Application Programming Interfaces
DSIT	Department for Science, Innovation and Technology
HMG	His Majesty's Government
IPO	Intellectual Property Office
ITHC	IT Health Check
MIBI	Management Information / Business Information
NCSC	The National Cyber Security Centre
SME's	Subject Matter Experts

5 AIMS AND OBJECTIVES

5.1 IPO needs a modular approach to penetration testing, keeping the scope of testing to sub-sections of the estate and undertaking testing on an ongoing basis giving the following benefits:

- Penetration testing is undertaken more regularly, providing better visibility of vulnerabilities across the estate.
- Reported vulnerabilities will be fewer for each test, allowing easier prioritisation. Each sub-section of the estate will be assessed providing a realistic 'deadline' for remediation of identified issues.

5.2 Appoint a Potential Provider to undertake support to the IPO for a 3-year period. This will include our annual needs plus any ad-hoc requirements. Awarding this contract to a single Potential Provider ensures the continuity of service and audit of identified issues and their remedial actions.

5.3 IPO needs CHECK accredited penetration tests to be undertaken of its entire estate, including infrastructure, web applications and APIs, external surface,

networking equipment, firewall rules, cloud architecture and Identity and Access Management solutions.

- 5.4** It is anticipated that the potential provider will perform all services remotely from its own offices or working from home as appropriate. Any travel and subsistence costs must be borne by the successful supplier.

6 THE REQUIREMENT

6.1 General Requirements & Methodology

- 6.2 Scope:** The IPO technical experts should work with the Potential Provider to clearly define the scope of the penetration testing, including the target systems and networks within IPO's IT environment that should be tested. Additionally, with the Potential Provider's advice, they should specify any specific applications or components that should be tested, such as those containing sensitive data or critical systems.
- 6.3 Methodology:** Performed tests must be rigorous and effective, ensuring a wide range of system attacks are simulated and include old and new methodologies. The potential Provider must:
- Deploy a structured process and plan, developed by SME's while specifying the methodology that should be used for the testing.
 - The testing team provided by the Potential Provider must be experienced in performing testing in accordance with the CHECK scheme, which is a UK government-backed framework for penetration testing.
 - Ensure that the testing team is familiar with the IPO's systems and network architecture to tailor the testing methodology.
- 6.4 Testing types:** Clearly specify the types of testing that should be conducted, such as external or internal testing, network testing, application testing, or social engineering testing. Specify which systems and networks the testing should focus on, such as critical systems or systems that hold sensitive data. Clearly specify risk management associated with potential system failure, system and network load and exposure of sensitive data.
- 6.5 Reporting:** Produce insightful, structured, practical, and easy to read reports, engaging with senior management in business terms, resolving issues with IT service providers, and addressing global risk management issues. The report should also include remediation suggestions and prioritise the vulnerabilities by risk severity.
- 6.6 Qualifications:** The testing team must be experienced in performing testing in accordance with the NCSC's CHECK scheme and hold SC (Security Cleared) clearance. Additionally, ensure that the testing team has experience in testing similar systems or applications and has familiarity with the regulations that the IPO complies with.
- 6.7 Legal considerations:** Ensure that the penetration testing contract includes provisions for compliance with relevant laws and regulations, such as data

protection laws, United Kingdom government policy and that the testing is conducted ethically and responsibly. Additionally, specify that the testing team should not disrupt the normal operations of the IPO during the testing and shall not compromise data protection requirements and or sensitive data.

- 6.8 Relationship: Co-develop security improvement strategies and programmes, recommending countermeasures to both address vulnerabilities and prevent them from occurring or re-occurring. Provide on-going advice and insights on how to manage systems effectively over time as part of a trusted relationship. Provide assurance remediated vulnerabilities discovered will 'secure' systems.

6.9 Specific Requirements:

- 6.10 The IPO requires that an IT Health Check (ITHC) be conducted as part of the NCSC specified and managed CHECK scheme, providing external assurance that the IT system's setup and configuration meets the desired HMG assurance level. The testing team should be experienced in conducting ITHCs and familiar with the IPO's systems and network architecture. The deliverable for this requirement will be an ITHC report detailing the assessment results, including vulnerabilities identified and remediation suggestions.
- 6.11 The IPO requires that penetration testing be conducted for existing systems applications related to Patents, Designs, Trademarks, and Application Control. The testing team should identify and prioritise vulnerabilities, provide remediation suggestions, and ensure compliance with relevant laws and regulations. The deliverable for this requirement will be a penetration testing report detailing the assessment results, including vulnerabilities identified and remediation suggestions. The report should include details of the agreed scope for easy reference. Reports should be received within 2 weeks of testing.
- 6.12 The IPO requires that comprehensive penetration testing be conducted for transformation projects involving REDACTED. The Potential Provider's testing team should identify and prioritise vulnerabilities, provide remediation suggestions, and ensure compliance with relevant laws and regulations. The deliverable for this requirement will be a penetration testing report detailing the assessment results, including vulnerabilities identified and remediation suggestions. The report should include details of the agreed scope for easy reference. Reports should be received within 2 weeks of testing.
- 6.13 The IPO requires that a build review be conducted monthly of up to three randomly sampled servers or workstations, where appropriate, evaluating their setup and configuration and identifying any security risks or vulnerabilities. The deliverable for this requirement will be a build review report detailing the assessment results, including vulnerabilities identified and remediation suggestions. Reports should be received within 2 weeks of testing.
- 6.14 REDACTED. The testing team should identify any potential security gaps and make remediation suggestions. The deliverable for this requirement will be a

- report detailing the assessment results, including vulnerabilities identified and remediation suggestions. Reports should be received within 2 weeks of testing.
- 6.15 The IPO requires that a code review be conducted to identify potential vulnerabilities in the source code of applications used in the IPO's systems. The Potential Provider's testing team should provide remediation suggestions and ensure compliance with relevant laws and regulations. The deliverable for this requirement will be a code review report detailing the assessment results, including vulnerabilities identified and remediation suggestions. Reports should be received within 2 weeks of testing.
- 6.16 The IPO requires testing that will cover both internal and external elements. This includes an external penetration test of IPO internet facing assets, "outside to in" testing, IP address ranges from the internet, internal penetration testing of the network DMZs (De-Militarised Zones), network external and internal layers, and access layer. It also includes a wireless assessment of the wireless networks as presented at Concept House, Newport. Please note future roadmap plans may change certain elements of our current network. Months 7-12 will be retesting to validate remediations.
- 6.17 Note: All systems connected to the IPO or other government networks will undergo an annual mandated IT Health Check (ITHC) as part of the testing process. The testing approach follows a modular structure, covering various elements such as external and internal penetration testing, network components, and wireless assessment. The deliverable for the ITHC will be multiple detailed reports identifying vulnerabilities and recommended actions for improvement. Reports should be received within 2 weeks of testing. This ensures manageability and a comprehensive testing process for all systems on an annual basis.
- 6.18 **Time Requirements:**
- 6.19 The IPO requires a three-year engagement, which is estimated to consist of 152 days for year 1, 122 days for year 2, and 122 days for year 3 on a call-off basis, with no commitment to use any of these days, equating to a combined total of 396 days over 3 years. This is an estimated number of days based on prior experience and the potential provider would need to be flexible on the number of days and the occasions when the provider is required. This will allow the IPO to have dynamic flexibility on all systems and resources that require testing and the potential supplier to conduct thorough and comprehensive testing across all systems and ensure that all identified vulnerabilities are addressed with recommended remediations.
- 6.20 All pre-live and beta projects must undergo a testing cycle consisting of test-remediate-test. This is to ensure that all vulnerabilities are identified, remediated, and validated before the system goes live.
- 6.21 All products, both live and pre-going live, must undergo NCSC CHECK testing certification. This is to ensure that all systems meet the required HMG assurance level and are compliant with relevant security standards. However, initial vulnerability testing and first assessments may not require CHECK certification.

This will be determined based on project scoping and timelines, in consultation with technical and security experts, and the testing team.

6.22 Note: The above time requirements are not fixed, but merely provided as an illustration of the need, and the IPO may adjust the times based on project needs and budget.

Existing Systems	Year 1 (days)	Year 2 (days)	Year 3 (days)	Comments
Patents	5	N/A	N/A	
Designs	5	5	5	
Trademarks	5	5	5	
Application control	5			
Build Testing	2	2	2	
Total	22	12	12	

External & Internal Testing	Year 1 (days)	Year 2 (days)	Year 3 (days)	Comments
Total	40	40	40	Mimic/improve current 6-month cycle test format

Transformation Testing	Year 1 (days)	Year 2 (days)	Year 3 (days)	Comments
Common Tech	25	15	15	
Data	10	10	10	
Manage	10	10	10	
Secure	10	10	10	
Research	10	10	10	
MIBI	10	5	5	
Buffer	15	10	10	Allows for unforeseen testing and retesting
Transformation Total	90	70	70	
Yearly Totals	152	122	122	Total Days = 396

7. PROJECT MILESTONES

7.1 The potential provider will note the following project milestones

Milestone	Description	Time
-----------	-------------	------

1	Start-up meeting via Microsoft Teams to gain additional information and context regarding IPO and to further clarify the scope.	Within 1 week of contract award
2	Provision of expert Penetration Testing support to Intellectual Property Office	From start of the contract to expiration of the contract
3	The successful Supplier shall ensure that all written reports are provided within agreed timescales and are clear, concise, jargon-free and solution oriented	Ongoing for the duration of contract
4	Testing is undertaken by members of the Potential Provider's Team at a level appropriate to team members' skills and experience and having due regard to customer's need for value for money.	Ongoing for the duration of contract
5	Key milestones will be identified within the scope of each test as agreed and communicated by the IPO.	Ongoing for the duration of contract

8.1 SERVICE LEVELS, KPIs & CUSTOMER SERVICE

8.2 The Authority will measure the quality of the Supplier's delivery by:

8.3 Critical Vulnerability Response Time SLA: The penetration testing vendor shall acknowledge and initiate the investigation of critical vulnerabilities discovered to the IPO team within 24 hours of discovery.

8.4 Testing Completion SLA: The penetration testing vendor shall complete all agreed-upon testing activities within the times specified in the scope and pre-engagement.

8.5 Secure Report Delivery and Classification SLA: The successful supplier shall securely share all testing reports with the IPO team using approved means to be agreed between the successful supplier and the IPO, such as guest accounts in Microsoft Teams. The reports shall be appropriately marked with the current classification scheme, following the IPO's requirements and guidelines which will be shared with the successful supplier upon contract award.

- 8.6 Contract Review meetings:** These shall be held annually as a minimum; however, the successful supplier will be required to attend contract review meetings as and when required by the Authority. Any face-to-face attendance shall be at the successful Supplier's own expense.

KPIs:

8.7 Customer Satisfaction:

- 8.8** Regular surveys or feedback sessions will assess the satisfaction level of the IPO team with the vendor's services. This includes collaboration through Microsoft Teams and the secure sharing of reports, ensuring a positive and efficient working relationship.

8.9 Quality of Reporting:

- 8.10** Continually assess the clarity, comprehensiveness, and organisation of the vendor's testing reports. Includes criteria such as adherence to the reporting template, report filetype, inclusion of detailed vulnerability descriptions, clear remediation guidance, and overall report presentation.

8.11 False Positive Rate KPI:

- 8.12** The penetration testing vendor will maintain a low false positive rate in their testing for the IPO, minimising the percentage of reported vulnerabilities later determined as false positives. This ensures accurate findings, reduces unnecessary efforts, and demonstrates precision in testing methodologies. Regular monitoring and reporting will allow the IPO to assess vendor performance.

9. OUTPUTS

- 9.1** Project deliverables are detailed above in Project Milestones, SLA's and KPI's are outlined in Sections 7 and 8.

10. QUALITY

- 10.1.** The Potential Provider must adhere to an excellent quality assurance process to ensure that the deliverables are of a high standard. This must include peer reviews of reports and appropriate and proportionate quality management means.

- 10.2.** Quality management standard ISO 9001.

- 10.3.** All testers require CHECK accreditation or to be supervised/overseen by an individual with CHECK assurance.

11. TIMINGS

- 11.1** The Potential Provider will provide attesting reports in the timescales agreed with the IPO.

12. RESOURCES

- 12.1** The potential provider must be able to scale resources appropriately to ensure timely delivery of contract requirements while also maintaining an appropriate balance between such scaling and the cost of the testing services to the IPO.
- 12.2** The Potential Provider will need to provide sufficient resource to achieve the required outcomes within the period of the contract.
- 12.3** The Potential Provider will have access to individuals within the IPO who will collaborate on the testing.
- 12.4** The working day will be a minimum of 8 hours. This is defined as the hours spent by the Potential Provider's Personnel properly working on the provision of the Services including time spent travelling (other than to and from the successful Supplier's offices, or to and from the Sites) but excluding lunch breaks.

13. VOLUMES

- 13.1** The IPO does not guarantee that the Potential Provider will be given any volume of work throughout the duration of the Contract.

14. SECURITY REQUIREMENTS & CONFIDENTIALITY

- 14.1** Confidentiality: The Potential Provider will comply with Clause 15 of the contract terms and conditions in respect of all work conducted for the customer.

15. SUSTAINABILITY

- 15.1** The IPO has a responsibility to act and to support nature, the environment, and its vital contributions to biodiversity. The successful Supplier is required to act in sustainable manner in the delivery of the Contract, particularly in terms of eliminating waste, reducing travel, and minimising energy consumption. The successful Supplier must comply with all current legislation regarding sustainability and legislation introduced or amended during the period of the contract pertaining to this.
- 15.2** This must include compliance with the Modern Slavery Act 2015 and the Climate Change Act 2008.

16. CONTINUOUS IMPROVEMENTS

- 16.1** The IPO expects the penetration testing vendor to demonstrate a commitment to continuous improvement in the delivery of the required services throughout the duration of the contract. The vendor is encouraged to proactively present innovative ways of working and improvements during regular contract review meetings, which can be conducted on an annual at a minimum, or as and when required by the Authority. Any proposed changes to the delivery of services should be communicated to the IPO for review and agreement before implementation. By fostering a culture of continuous improvement, the vendor can contribute to the ongoing enhancement of the penetration testing services provided to the IPO, ensuring optimal effectiveness and efficiency in identifying and addressing security vulnerabilities.
- 16.1** The successful Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

- 16.2** The successful Supplier should present new ways of working to the Authority during Contract review meetings.
- 16.3** Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

17. PAYMENT

- 17.1** Payment will only be made on satisfactory delivery of the agreed Penetration Testing services.
- 17.2** Before payment, any invoices that are received must include a detailed breakdown of the work completed, the associated costs and a quote reference number.
- 17.3** All invoices must quote a relevant IPO Purchase Order and Contract reference number and be emailed to REDACTED
- 17.4** Payment will be made within 30 days of receipt of invoice.

Order Schedule 22 – Secret Matters

Associated definitions:

In this Order Schedule 22, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Document"	includes specifications, plans, drawings, photographs and books;
"Secret Matter"	means any matter connected with or arising out of the performance of this Order Contract which has been, or may hereafter be, by a notice in writing given by the Customer to the Supplier be designated 'top secret', 'secret', or 'confidential';
"Servant"	where the Supplier is a body corporate shall include a director of that body and any person occupying in relation to that body the position of director by whatever name called.

1. Disclosure

- 1.1** The Supplier shall not, either before or after the completion or termination of this Order Contract, do or permit to be done anything which it knows or ought reasonably to know may result in information about a Secret Matter being:
- 1.1.1 without the prior consent in writing of the Buyer, disclosed to or acquired by a person who is an alien or who is a British subject by

virtue only of a certificate of naturalisation in which his name was included;

1.1.2 disclosed to or acquired by a person as respects whom the Buyer has given to the Supplier a notice in writing which has not been cancelled stating that the Buyer requires that Secret Matters shall not be disclosed to that person;

1.1.3 without the prior consent in writing of the Buyer, disclosed to or acquired by any person who is not a Servant of the Supplier; or

1.1.4 disclosed to or acquired by a person who is an employee of the Supplier except in a case where it is necessary for the proper performance of this Order Contract that such person shall have the information.

2. Safeguarding

- 2.1 Without prejudice to the provisions of Paragraph 1, the Supplier shall, both before and after the completion or termination of this Order Contract, take all reasonable steps to ensure:

2.1.1 no such person as is mentioned in Paragraph 1.1, 1.1.1 or 1.1.2, thereof shall have access to any item or Document under the control of the Supplier containing information about a Secret Matter except with the prior consent in writing of the Buyer;

2.1.2 that no visitor to any premises in which there is any item to be supplied under this Order Contract or where Goods are being supplied shall see or discuss with the Supplier or any person employed by him any Secret Matter unless the visitor is authorised in writing by the Buyer so to do;

2.1.3 that no photograph of any item to be supplied under this Order Contract or any portions of the Goods shall be taken except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, and that no such photograph shall, without such consent, be published or otherwise circulated;

2.1.4 that all information about any Secret Matter and every Document, model or other item which contains or may reveal any such information is at all times strictly safeguarded, and that, except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, no copies of or extracts from any such Document, model or item shall be made or used and no designation of description which may reveal information about the nature or contents of any such Document, model or item shall be placed thereon; and

2.1.5 that if the Buyer gives notice in writing to the Supplier at any time requiring the delivery to the Customer of any such Document, model or item as is mentioned in Paragraph 2.1.4, that Document, model or item (including all copies of or extracts therefrom) shall forthwith be

delivered to the Buyer who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

3. Decision of the Buyer

- 3.1 The decision of the Buyer on the question whether the Supplier has taken or is taking all reasonable steps as required by the foregoing provisions of this Order Schedule 22 shall be final and conclusive.

4. Particulars of People

- 4.1 If and when directed by the Buyer, the Supplier shall furnish full particulars of all people who are at any time concerned with any Secret Matter.

5. Official Secrets Act

- 5.1 If and when directed by the Buyer, the Supplier shall secure that any person employed by it who is specified in the direction, or is one of a class of people who may be so specified, shall sign a statement that he understands that the Official Secrets Act, 1911 to 1989 and, where applicable, the Atomic Energy Act 1946, apply to the person signing the statement both during the carrying out and after expiry or termination of the Order Contract.

6. Information concerning the Contract

- 6.1 If, at any time either before or after the expiry or termination of this Order Contract, it comes to the notice of the Supplier that any person acting without lawful authority is seeking or has sought to obtain information concerning this Order Contract or anything done or to be done in pursuance thereof, the matter shall be forthwith reported by the Supplier to the Buyer and the report shall, in each case, be accompanied by a statement of the facts, including, if possible, the name, address and occupation of that person, and the Supplier shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any person employed by it, that person shall forthwith report the matter to the Supplier with a statement of the facts as aforesaid.

7. Duty to observe obligations

- 7.1 The Supplier shall place every person employed by it, other than a Sub contractor, who in its opinion has or will have such knowledge of any Secret Matter as to appreciate its significance, under a duty to the Supplier to observe the same obligations in relation to that Secret Matter as are imposed on the Supplier by Paragraphs 1 and 2 and shall, if directed by the Buyer, place every person who is specified in the direction or is one of a class of people so specified, under the like duty in relation to any Secret Matter which may be specified in the direction, and shall at all times use its best endeavours to ensure that every person upon whom obligations are imposed by virtue of this Order Schedule 22 observes the said obligations, and the Supplier shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the

said obligations, report the facts to the Supplier with all necessary particulars.

8. Sub-Contract Obligations

- 8.1 The Supplier shall, if directed by the Buyer, include in the Sub-Contract provisions in such terms as the Buyer may consider appropriate for placing the Sub-Contractor under obligations in relation to secrecy and security corresponding to those placed on the Supplier by this Order Schedule 22, but with such variations (if any) as the Buyer may consider necessary. Further the Supplier shall:

8.1.1 give such notices, directions, requirements and decisions to its Sub Contractors as may be necessary to bring the provisions relating to secrecy and security which are included in Sub-Contracts under this Order Schedule 22 into operation in such cases and to such extent as the Buyer may direct;

8.1.2 if there comes to its notice any breach by the Sub-Contractor of the obligations of secrecy and security included in their Sub-Contracts in pursuance of this Order Schedule 22, notify such breach forthwith to the Customer; and

8.1.3 if and when so required by the Buyer, exercise its power to determine the Sub-Contract under the provision in that Sub-Contract which corresponds to Paragraph 11.

9. Information to the Buyer

- 9.1 The Supplier shall give the Buyer such information and particulars as the Buyer may from time to time require for the purposes of satisfying the Buyer that the obligations imposed by or under the foregoing provisions of this Order Schedule 22 have been and are being observed and as to what the Supplier has done or is doing or proposes to do to secure the observance of those obligations and to prevent any breach thereof, and the Supplier shall secure that a representative of the Buyer duly authorised in writing shall be entitled at reasonable times to enter and inspect any premises in which anything is being done or is to be done under this Order Contract or in which there is or will be any item to be supplied under this Order Contract, and also to inspect any Document or item in any such premises or which is being made or used for the purposes of this Order Contract and that any such representative shall be given all such information as he may require on the occasion of, or arising out of, any such inspection.

10. Exclusion

- 10.1 Nothing in this Order Schedule 22 shall prevent any person from giving any information or doing anything on any occasion when it is, by virtue of any enactment, the duty of that person to give that information or do that thing.

11. Grounds for Termination

- 11.1 If the Buyer shall consider that any of the following events has occurred:

11.1.1 that the Supplier has committed a breach of, or failed to comply with any of, the foregoing provisions of this Order Schedule 22; or

11.1.2 that the Supplier has committed a breach of any obligations in relation to secrecy or security imposed upon it by any other contract with the Buyer, or with any department or person acting on behalf of the Crown; or

11.1.3 that by reason of an act or omission on the part of the Supplier, or of a person employed by the Supplier, which does not constitute such a breach or failure as is mentioned in Paragraph

11.1.4 information about a Secret Matter has been or is likely to be acquired by a person who, in the opinion of the Buyer, ought not to have such information;

11.1.5 and shall also decide that the interests of the state require the termination of this Order Contract, the Buyer may by notice in writing terminate this Order Contract forthwith.

12. Buyer Decision to Terminate

- 12.1 A decision of the Buyer to terminate this Order Contract in accordance with the provisions of Paragraph 11 shall be final and conclusive and it shall not be necessary for any notice of such termination to specify or refer in any way to the event or considerations upon which the Buyer's decision is based.

13. Supplier's notice

- 13.1 The Supplier may within five (5) Working Days of the termination of this Order Contract in accordance with the provisions of Paragraph 11, give the Buyer notice in writing requesting the Buyer to state whether the event upon which the Buyer's decision to terminate was based is an event mentioned in Paragraphs 11.1.1, 11.1.2 or 11.1.3 and to give particulars of that event; and
- 13.2 the Buyer shall within ten (10) Working Days of the receipt of such a request give notice in writing to the Supplier containing such a statement and particulars as are required by the request.

14. Matters pursuant to termination

- 14.1 The termination of this Order Contract pursuant to Paragraph 11 shall be without prejudice to any rights of either Party which shall have accrued before the date of such termination;
- 14.2 The Supplier shall be entitled to be paid for any work or thing done under this Order Contract and accepted but not paid for by the Buyer at the date of such termination either at the price which would have been payable under this Order Contract if the Order Contract had not been terminated, or at a reasonable price;
- 14.3 The Buyer may take over any work or thing done or made under this Order Contract (whether completed or not) and not accepted at the date of such

termination which the Buyer may by notice in writing to the Supplier given within thirty (30) Working Days from the time when the provisions of this Order Schedule 22 shall have effect, elect to take over, and the Supplier shall be entitled to be paid for any work or thing so taken over a price which, having regard to the stage which that work or thing has reached and its condition at the time it is taken over, is reasonable. The Supplier shall in accordance with directions given by the Buyer, deliver any work or thing taken over under this Paragraph 14.3, and take all such other steps as may be reasonably necessary to enable the Buyer to have the full benefit of any work or thing taken over under this Paragraph 14.3 ; and

- 14.4 Save as aforesaid, the Supplier shall not be entitled to any payment from the Buyer after the termination of this Order Contract.

15. Rights & Obligations after Termination

- 15.1 If, after notice of termination of this Order Contract pursuant to the provisions of Paragraph 11:
- 15.1.1 the Buyer shall not within ten (10) Working Days of the receipt of a request from the Supplier, furnish such a statement and particulars as are detailed in Paragraph 13.1; or
 - 15.1.2 the Buyer shall state in the statement and particulars detailed in Paragraph 13.2 that the event upon which the Buyer's decision to terminate this Order Contract was based is an event mentioned in Paragraph.11.1.3,
 - 15.1.3 the respective rights and obligations of the Supplier and the Buyer shall be terminated in accordance with the following provisions:
- 15.2 the Buyer shall take over from the Supplier at a fair and reasonable price all unused and undamaged materials, bought-out parts and components and articles in course of manufacture in the possession of the Supplier upon the termination of this Order Contract under the provisions of Paragraph 11 and properly provided by or supplied to the Supplier for the performance of this Order Contract, except such materials, bought-out parts and components and articles in course of manufacture as the Supplier shall, with the concurrence of the Buyer, elect to retain;
- 15.3 the Supplier shall prepare and deliver to the Buyer within an agreed period or in default of agreement within such period as the Buyer may specify, a list of all such unused and undamaged materials, bought-out parts and components and articles in course of manufacture liable to be taken over by or previously belonging to the Buyer and shall deliver such materials and items in accordance with the directions of the Buyer who shall pay to the Supplier fair and reasonable handling and delivery charges incurred in complying with such directions;
- 15.4 the Buyer shall indemnify the Supplier against any commitments, liabilities or expenditure which are reasonably and properly chargeable by the Supplier in connection with this Order Contract to the extent to which the said commitments, liabilities or expenditure would otherwise represent an

unavoidable loss by the Supplier by reason of the termination of this Order Contract;

- 15.5 if hardship to the Supplier should arise from the operation of this Paragraph 15 it shall be open to the Supplier to refer the circumstances to the Buyer who, on being satisfied that such hardship exists shall make such allowance, if any, as in its opinion is reasonable and the decision of the Buyer on any matter arising out of this Paragraph 15.5 shall be final and conclusive; and
- 15.6 subject to the operation of Paragraphs 15.2, 15.3, 15.4, and 15.5 termination of this Order Contract shall be without prejudice to any rights of either party that may have accrued before the date of such termination.