Crown Commercial Service

G-Cloud 9 Call-Off Contract

This Call-Off Contract for the G-Cloud 9 Framework Agreement (RM1557ix) includes:

Part A - Order Form

Digital Marketplace service ID number:	C-Track Case Management System 181395018176810 C -Track E-Filing 745573013922249 C-Track Implementation Service 801082969660773 C-Track Training Services 394946037811907
Call-Off Contract reference:	CON_15637
Call-Off Contract title:	C-Track Cloud Software As a Service
Call-Off Contract description:	Civil Case Management System for the Royal Courts of)ustice, four Chambers of the Upper Tribunal and Employment Appeal Tribunal
Start date:	01/06/2018
Expiry date:	31/05/2020
Call-Off Contract value:	[REDACTED]
Charging method:	Monthly in arrears
Purchase order number:	TBC upon contract signature

This Order Form is issued under the G-Cloud 9 Framework Agreement (RM1557ix).

Buyers can use this order form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with **square brackets.**

From: the Buyer	[REDACTED] Buyer's main address: Ministry of Justice 102 Petty France 10''' Floor

	London SW1H9AJ
To: the Supplier	[REDACTED] Supplier's address: Thomson Reuters (Professional) UK Limited 5 Canada Square Canary Wharf London E145AQ Company number: 016749
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title: Commercial Manager [REDACTED]
For the Supplier:	Title: Director, Service Delivery [REDACTED]

Call-Off Contract term

Start date:	This Call-Off Contract starts on 01/06/2018 and is valid for twenty-four (24) months.
Encling (termination):	The notice period needed for Ending the Call-Off Contract is at least ninety (90) Working Days from the date of written notice for disputed sums or at least thirty (30) days from the date of written notice for Ending without cause.
Extension period:	[REDACTED]

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 2 - Cloud Sofrware Lot 3 - Cloud support
G-Cloud services required:	The Services to be provided by the Supplier under the above Lots are listed in Framework Section 2 and outlined below: The anticipated volumes provided below are based on a forecast provided by the Buyer as set out in Annex 2 to Schedule 1. The Parties accept that these are indicative volumes only as G-Cloud Services are commodity based, pay-as-you go cloud services. C-Track Case Management System 181395018176810 The anticipated volume of all services under this contract for a twenty-four (24) month period are: 165,910 cases per annum. **C-Track** E-Filing **745573013922249** The anticipated volume of all services under this Call-Off Contract for a twenty-four (24) month period are: 165,910 cases per annum. C-Track Implementation Service 801082969660773 Tables 3 to 4 in Schedule 2 of this Call-Off Contract provides an indicative estimate provided by the Supplier for delivering the High-Level Requirements as defined in Annex 1 to Schedule 1. [REDACTED]
Additional **services:**	None

Location:	**SUPPLIER'S PRINCIPAL LOCATIONS** Product Management & Development 5 Canada Square, Canary Wharf, London El4 SAQ **Datacentres** 1 Paul Julius Close, Blackwall Way, Poplar, Greater London, El4 2EH (Production) 18 Brunel Way, POlS STX Portsmouth, Hampshire, United Kingdom (Disaster Recovery) **BUYER'S PRINCIPAL LOCATIONS** The Services will be delivered to: • Royal Courts ofJustice, Fetter Lane, London, EC4A lNL • Rolls Building, Queens Bench and Upper Tribunal chambers for Administrative Appeals, Tax and Land, Strand, London, WC2A 2LL • Upper Tribunals in Field House, 15-25 Breams Buildings, London EC4A lDZ • Employment Appeals Tribunal, 2nd Floor, Fleetbank House, 2-6 Salisbury Square, London EC4Y *BAE* • **District registries and local administrative offices** Note: • Field and Fleetbank House based teams may move to the other London Offices. • Due to the nature of the Buyer's Reform programme and the size of change **happening in the organisation, the locations set out here may not remain the same** but the number of jurisdictions being delivered will not change.
Qµality standards:	The quality standards required for this Call-Off Contract are defined in the Service Definition for this service as published on the Digital Marketplace.
Technical standards:	The technical standards required for this Call-Off Contract are defined in the Service Agreement for this service as published on the Digital Marketplace.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are defined in the Service Definition and Terms of Service for this service as published on the Digital Marketplace.
Onboarding:	The onboarding plan ('Implementation Plan') for this Call-Off Contract is to be agreed between both parties in accordance with Schedule 1 (Implementation Services and Implementation Plan) of this Call-Off Contract.
Offboarding:	The oftboarding plan for this Call-Off Contract is to be agreed between both parties, in accordance with Schedule 1 (Exit) of this Call-Off Contract.
Limit on Parties' liability:	[REDACTED]
Insurance:	[REDACTED]

Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than ninety (90) consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. The Audit requirements for this Call-Off Contract are set out in the Buyer's Non-Functional Requirements as defined in Annex 1 to Schedule 1 of this Call-Off Contract.
Buyer's responsibilities:	The Buyer is responsible for: • The Buyer will supply, by agreement the necessary members of their technical and operational staff to work with the Supplier's service delivery team in the provision of support and maintenance of the CE-File Service and implementing changes to the CE-File Service. • The Buyer will appoint a representative to act as a point of contact for liaising between the Supplier's support team, and the Buyer's operations team (role and responsibilities defined in Annex 1 of Schedule 9 of this Call-Off Contract). • The Buyer will provide end-user training using the training materials provided by Supplier, and such supplemental materials created by the Buyer. The Supplier can provide additional training and training materials and collateral (e.g. marketing and other communications material) as agreed with the Buyer, subject to payment by the Buyer of such additional fees at the Supplier's agreed time and materials rates detailed in Schedule 2 to this Call-Off Contract. • The Buyer will provide first line support (as defined in the Operational Working Agreement in Schedule 9 to this Call-Off Contract through a service desk, for Users of the CE-File Service, using reasonable endeavours to resolve functional support issues raised by Users directly. The Buyer agrees that the Supplier's support services are not intended to resolve incidents that derive from User error, lack of User training and other such incidents that are unrelated to loss of functionality, loss of service or bugs and errors in the Services. The Parties will monitor the number of such incidents **being reported each month, and if such incidents are trending on the increase, or are** stabilising at a level that is mutually agreed to be materially affecting the Supplier's ability to resolve incidents related to loss of functionality, loss of service or bugs and errors, the Buyer agrees to take reasonable steps to reduce such incidents, including providing relevant training to its Users or procuring the provision of additional Training Services from Supplier. • The Buyer shall submit all incidents requiring 2nd and 3rd line support to the Supplier via the Buyer's Service Desk, reasonably promptly, providing such information, as defined in the Operational Working Agreement (detailed in Schedule 9 to this Call-Off Contract, that may be reasonably required by Supplier to resolve such incidents,

	including such information to enable the Supplier to replicate the issue where applicable. The Buyer understands that the Supplier may not be able to resolve incidents which cannot be replicated by Supplier in its pre-production environments **(provided such pre-production environments replicate its production environments in** all material respects) however, the Supplier shall work with the Buyer to reach a mutually agreeable solution. • The Buyer will provide the Supplier with access to suitably qualified personnel of the Buyer's third-party contractors that the Supplier reasonably requires (including but not limited to network connectivity and service desk). • Where feasible the Buyer will allow the Supplier access to the Buyer's premises and communications facilities and provide the Supplier with reasonable work space and storage and other normal and customary facilities to fulfil their obligations to resolve incidents. The Supplier shall not rely on the Buyer being able to provide this. • The Buyer will provide the same standard of care in relation to the CE-File Service (and associated Documentation) that it applies to its own products, data or **documentation of like value to its business and return any defective Documentation or** attest in writing to the destruction of the same, as directed by the Supplier. • The Buyer will procure the accurate and timely performance of the responsibilities of the Buyer set out in Operational Working Agreement detailed in Schedule 9 to this Call-Off Contract and those subsequently agreed to be undertaken pursuant to the **Government Procedures.** • The Buyer will carry out its responsibilities under this Section 'Buyer's Responsibilities' exercising that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from an experienced purchaser of information technology services of the level of complexity of the G-Cloud Services.
Buyer's equipment:	The Buyer's equipment to be used with this Call-Off Contract includes: • Where feasible the Buyer will provide and maintain Internet Access in the Buyer's buildings for its Users to connect to the Services, and provide the Supplier with access to the same. The Supplier shall not rely on the Buyer being able to provide this. • The Buyer understands that the Services support the relevant versions of third party browsers and other such third-party sofrware, as such policy may change from time to **time.** • Buyer shall ensure that its Users are provided with devices installed with applicable browsers and sofrware. The Supplier will provide the Buyer with at least six (6) months' notice of any withdrawal of support for specific versions of such third-party **browsers and software.**

Supplier's information

Subcontractors or partners:	The following is a list of the Supplier's Subcontractors or Partners. [REDACTED]

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method:	The payment method for this Call-Off Contract is BACS.
Payment profile:	The payment profile for this Call-Off Contract is monthly in arrears.
Invoice details:	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within thirty (30) days of receipt of a valid invoice. OJ,.arterly Invoice Process (True Up) At the end the Reporting Period the Parties will undertake a true up to verify the amount paid aligns with the actual owed for that Reporting Period based on actual substantive case volumes and the pricing in the Pricing model set out in Schedule 2 of this Call-Off Contract. The Supplier will produce a report of substantive case volumes from CE-File for the Reporting Period for review and agreement by the Parties by the 10th working days of the end of a Reporting Period. The Supplier will raise a Quarterly Report by the 10th working day of the end of the Reporting Period which details the amount paid for that Reporting Period compared to the actual amount owed for that Reporting Period and will detail any credit owed to the Buyer. The Quarterly Report should be sent to the Buyer for approval. The Buyer shall approve or

	reject the Quarterly Report within three (3) working days. If the Supplier owes the Buyer a credit this will be credited back to the Buyer in the next **invoice period.**
Who and where to send invoices to:	**Invoices will be sent to:** Ministry of Justice (HMCTS) PO Box 745, Newport, Gwent, Wales, NPlO 8FZ Or: Email: apinvoices-CTS-u@sscl.gse.gov.uk [REDACTED]
Invoice infonnation required - for example purchase **order, project reference:**	**All invoices must include:** Call-Off Contract Reference Purchase Order Number
Invoice freauency:	The invoice will be sent to the Buyer monthly.
Call-Off Contract value:	[REDACTED]
Call-Off Contract charges:	[REDACTED]

Additional buyer terms

Performance of the service and deliverables:	Schedule 1 of this Call-Off Contract includes information on the performance of the services and deliverables.
Supplemental requirements in addition to the Call-Off **terms:**	Within the scope of the Call-Off Contract, the Supplier accepts that: The rate card detailed in Schedule 2 is fully inclusive of all travel and subsistence costs to the Royal Courts of Justice ('Base location') and Upper Tribunal or other offices in London. For any work performed at a location different to that of the Base location and London (outside of the M25), all reasonable travel and expenses costs shall be met in accordance with the rates set out in the Mo) travel and subsistence policy. All expenses will require prior approval from HMCTS before being reimbursed [REDACTED]

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557ix.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]
Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Schedule 1 - Services

This Call-Off Schedule I specifies the:

1. Service Definitions contained within this Schedule 1
2. Service Support
3. Implementation Services and Implementation Plan (including data migration)
4. **Training Provision**
5. Exit

Annex I - High-Level Requirements
Annex 2 - In-Scope Courts and Tribunals
Annex 3 - Service Levels
Annex 4 - Indicative High-Level Implementation Plan
Annex 5 - Indicative Discovery Plan
Annex 6 - Example Training Deliverables

1. SERVICE DEFINITIONS

The following definitions shall apply to this Schedule 1:

"CE-File Service"	means the CE-File Service, on the date of this Agreement provided by Supplier under this Call-Off Contract, and such changes to such CE-File Service as agreed between the Parties pursuant to this Agreement.
"Discovery Plan"	means the detailed plan that the Parties shall follow to undertake the Discovery phase and define the Prioritised Requirements List, as set out in this Schedule 1 (Implementation).
"Discovery"	means the initial onboarding engagement with the Buyer to produce and agree **a set of requirements with implementation timelines.**
"Exit Plan"	means the detailed plan that the Parties shall follow to exit the CE-File Services upon a termination of this Call-Off Contract, as agreed in accordance with this Schedule 1 (Exit).
"Exit Services"	means the services provided by the Supplier to exit the provision of the **Services, and provide migration assistance, as agreed in the Exit Plan.**
"High Level Requirements"	**means the functional and non-functional requirements set out in Annex 1 A to** this Schedule 1.
"HMCTS"	means Her Majesty Courts and Tribunal Service.
"Hypercare Support"	A period when the Supplier will closely monitor customer service, data Integrity and the smooth functioning of the implemented application outside of the support SLAs.
"Implementation Plan"	means the detailed plan that the Parties shall follow to change the CE-File **Service in a prioritised manner in accordance with the Prioritised Requirements List.**
"Implementation Services''	means the Supplier's services to change the CE-File Service and onboard the In-Scope Courts and Tribunals in accordance with the Implementation Plan
"In-Scope Courts and Tribunals"	means the in-scope jurisdictions and chambers listed in Annex 2 to this Schedule l; the case volumes set out in Annex 2 to this Schedule 1 are **indicative of the annual case volumes.**
"Jurisdiction"	means each jurisdiction within the In-Scope Courts and Tribunals;
"Milestone"	means an event or task described in the Implementation Plan.
"Prioritised Requirements List"	**means the Buyer's list of prioritised requirements, categorised by "must-have", "should-have", "could-have" and "won't-have", for the CE-File Service to meet** the needs of the In-Scope Courts and Tribunals, and their users, as agreed **between the Parties, from time to time, in accordance with the Governance** Mechanism set out in this Schedule 1 (Implementation).
"Reform Programme"	means a HMCTS programme to modernise and transform the Courts and Tribunals system.
"Service Levels"	means the levels of service for providing Service Support, as set out in Annex 3 to this Schedule 1
"Service Support"	means the services to support CE-File Service, as described in this Schedule 1 (Service Support), in accordance with the Service Levels.
"Training Services"	means the Supplier's services to train the Buyer's users in accordance with the Implementation Plan.

SERVICES

Under this Call-Off Schedule, the Supplier shall:

- provide the CE-File Service and the Service Support in accordance with the Service Levels;
- provide the Implementation Services, and change the CE-File Service, as agreed between the parties pursuant to the **Governance Mechanism; and**
- **provide the Training Services as agreed between the parties pursuant to the Governance Mechanism; and** at the request of the Buyer in the event of termination of this Call Off Contract, provide Exit Services, as agreed between the parties pursuant to the Governance Mechanism in accordance with Schedule 1 (Implementation).

2. SERVICE SUPPORT

The Supplier's Service Support shall cover the following elements:

- Release Hypercare Support
- 2nd Level and 3rd Level Support;
- Incident and Change Management; and
- Hosting/Availability of the service

RELEASEHYPERCARESUPPORT

Each Jurisdiction will need to go through a formal acceptance into service process whereby it will move from project support into live support. For example, the Buyer will expect the Supplier to provide full support prior to transitioning 1st line calls to the Buyer's Service Desk.

The Supplier will provide Hypercare Support onsite for up to two (2) weeks following a release to allow the Supplier to triage any post release bugs, while the development team is still engaged to provide hot fixes.

The Buyer's !st Line Support provider will continue to provide 1st Level Support for the CE-File Service for internal users through a service desk to resolve functional support issues raised by users directly.

2ND AND 3RD LINE SUPPORT

Subject to the Buyer continuing to pay the annual charges for the CE-File Services, the Supplier will provide the following standard levels of support in relation to the Service:

- The provision of 2nd level and 3rd level incident resolution and the issuing of bug fixes on a prioritised basis in accordance with the Service Levels.
- With the exception of hot fixes that the Parties agree to release into the CE-File Service on an, as needed basis, the Supplier will provide no more than two (2) releases per year to maintain the CE-File Service in line with the C-Track core product {on a like for like functional basis), and to release bug fixes not released as hot fixes.
- The Buyer will also have the benefit of functional enhancements delivered through the ongoing investment by the Supplier in continual improvement in the C-Track product suite delivered through the product roadmap, as described below, subject to any charges for Specialist Cloud Services to release additional functionality not previously implemented to the Buyer.

INCIDENTS AND CHANGE MANAGEMENT

Incident Management

In the event of an incident, the Supplier will manage to resolution any escalations from the Buyer in accordance with the Supplier's Incident Management Process document (available upon request), which has previously been agreed with the Buyer. In the event of a Major incident with impact on the Buyer's Service Desk, the Supplier will advise the CE-File admin group accordingly

The Supplier's Incident Management team will have responsibility for the following:

- **In the event of a major incident, organise and chair incident management calls**
- Providing the CE-File admin group with updates as requested

- Providing the CE-File admin group with confirmation of the Major incident resolution
- **Conducting major post incident reviews to ensure detailed analysis of the Incident occurs, and to ensure service improvement programmes are implemented**
- **Ensuring trends in incident occurrence are surveyed and reported via the monthly service report.**

Change Management

- The Parties will manage any change in accordance with the Change Management Process which has previously been agreed with the Buyer.
- Changes managed via the Supplier will be communicated to the HMCTS CE-File admin group
- If a Supplier change to CE-File is deemed to have potential impact on other Buyer systems then the Supplier will advise the HMCTS CE-File admin group.

Continual Improvement
The Supplier shall:

- manage a quality assurance processes in the run up to releases to reduce the likelihood of post release support **issues;**
- **manage the release of updates to their infrastructure to automate processes, where possible, to reduce the risk of human error; and**
- manage pro-active monitoring of the solution so that they are better able to spot the early warning signs of problems with the solution.

AVAILABILITY
The Supplier shall ensure that the CE-File Service:

- **is available for use over the Internet, and**
- performs to meet the loads expected (as set out in Annex 3 to this Schedule 1),

in accordance with the Service Levels

INFORMATION SECURITY AND QUALITY MANAGEMENT
The Supplier's Service Delivery Organisation shall have an established quality management system (QMS) in place that supports the CE-File Service which includes:

- DSDM as an industry standard agile project management arid delivery framework.
- Certified quality management system conformance to ISO 9001.
- Security certification conformance to ISO:27001:2005 for our data centre.
- Use of Jira as a development workflow tool and bug tracker.
- Development systems and governance to manage code quality and maintainability, including source control, **continuous integration, code quality test coverage and metrics.**
- A **test automation function that oversees the test automation framework and testing at all the various stages.**
- **A release management service to ensure releases go smoothly.**
- Service management aligning with ITIL best practices.
- **Data recovery systems to ensure availability.**
- **Usage and performance monitoring and tuning to understand and pro-actively alert on issues.**
- **Business continuity plans.**

The Supplier shall improve their processes continually, based on their own review and Buyers' feedback.

PRODUCT ROADMAP, RELEASE CYCLE AND OBSOLESCENCE POLICY

The Supplier has a fully funded product roadmap with a prioritised list of enhancements to the core C-Track product suite planned until 2018, with key releases being issued every quarter. Prioritisation and planning offeature releases will happen quarterly based on a combination of market and Buyer needs. Through the Supplier's account management **programme, they will recommend regular consultation with the Product Manager to ensure its future business needs are** captured and fed into the prioritisation process.

SOFI'WARE VERSION SUPPORT REVIEW POLICY & ROADMAP

Software Requirements Overview

- Application Server: The application server requires a fully patched OS, Java JDK, and Tomcat/Weblogic application **container.**
- Database Server: CE-File supports both SQL Server and Oracle databases. The OS for the server must be in the supported OS list and must also support the selected database server (e.g. SQL Server requires Windows).
- Client: The Buyer must support a fully patched version of the browsers listed below. No)RE or other plugins are **required in the browser.**

VERSION SUPPORT POLICY

The Supplier will review and assess new available software versions and products for inclusion on the supported software versions roadmap. The Supplier will notify existing clients of modifications to the support software versions roadmap.

- The Buyer may request expedited support coverage for new available software versions or products. When requested, the Supplier's product management team will provide a quote for services associated with corresponding system upgrade testing and development efforts.
- The Supplier will aim to provide up to six (6) months' notice of the withdrawal of support for third party software versions, and the withdrawal of any material functions or features in the product suite. Notwithstanding the **foregoing, if material features or functions are withdrawn from versions of the product suite, Supplier aims to replace** such features or functions with features or functions that deliver substantially the same capability in a different way. All such changes will be discussed in advance with the Buyer.

3. IMPLEMENTATION SERVICES AND IMPLEMENTION PLAN (Inclucling Data Migration)

Introduction
On the date of this Call-Off Contract:

- the Buyer has provided the Supplier with its functional and non-functional requirements for a service to meet the needs of the In-Scope Courts and Tribunals, in Annex 1 to this Schedule 1; and
- the Supplier has provided a response to the High-Level Requirements, the Supplier's responses are contained in Annex 1 to this Schedule I.
- The estimated On Boarding costs are set out in Schedule 2

The Parties agree to conduct an initial Discovery phase to validate the High-Level Requirements with users from the In-Scope Courts and Tribunals to define and agree a Prioritised Requirements List and Implementation Plan for changing the CE-File Service and onboarding new Jurisdictions within the In-Scope Courts and Tribunals onto the CE-File Service.

The Parties agree that the starting point for the Prioritised Requirements List is the High-Level Requirements. As the Parties undertake the Discovery phase, they shall validate the High-Level Requirements with users from the In-Scope Courts and Tribunals to define and agree the Prioritised Requirements List and Implementation Plan, working on the following principles:

- The High-Level Requirements are not a fixed set ofrequirements; as the Discovery phase progresses, requirements may be dropped or modified and new requirements may be added. As more understanding of the Buyer's requirements become available, the Supplier will be given the opportunity to update its estimates for delivering the Implementation Services and Training Services.
- The Buyer has an objective to deliver all of the In-Scope Courts and Tribunals on to the CE-File Service, as modified to meet the needs of the In-Scope Courts and Tribunals, and their users, within the term ofthis Call-OffContract, and subject to Call-Off Contract Value. The Parties will work together, in good faith, to agree the Prioritised Requirements List and Implementation Plan.

The Parties agree that the Prioritised Requirements List and Implementation Plan are intended to be "living" documents and subject to change in accordance with the Governance Mechanism.

The Parties agree that an initial version of the Prioritised Requirements List and Implementation Plan may be agreed prior to completion of the Discovery Plan to enable the Supplier to commence providing Implementation Services and/or Training Services for the first In-Scope Court or Tribunal to be onboarded onto the CE-File Service, and/or to make changes to the CE-File Service.

Progress against the Implementation Plan will be managed by the Delivery Board whose role is set in the Governance Mechanism.

Resourcing
The Supplier will provide a skilled team with extensive legal technology experience (business analysis, project management, training, software development, and integration capabilities) for the delivery of the CE-File Service.

During the initial roll-out of the CE-File Service, the Parties shall agree the co-location of the Supplier's delivery team alongside the Buyer's Project Team to ensure close collaboration on the project.

In line with the current delivery approach for ongoing service support of the CE-File services, the Supplier's Court Management Solutions team in the UK will be supported by their Sub-Contractors/ Delivery Partners as listed in the Order Form of this Call-Off Contract. The Sub-Contractors/ Delivery Partners will work under the control of the Supplier's Services Director and Lead Architect

GOVERNANCE MECHANISM

Delivery Board
The Delivery Board shall meet monthly with representatives to be agreed berween the Parties as set out in the Buyer's Terms of Reference.

The Delivery Board shall be responsible for the following:

- Be accountable individually and collectively for the success of the RC) & UT Reform project.
- Ensure resources are allocated effectively and arbitrate on any conflicts within the project.
- Ensure delivery of the mandatory business requirements, as signed off by the business users and agreed by the Delivery Board
- Ensure that timescales appear achievable.
- **Ensure that quality measures are sufficient.**
- Fulfil the quality assurance role within the project.
- Negotiate any problems berween the project and bodies external to the project.
- Ensure the project delivers value for money and monitor spend against the financial delegation and tolerance.
- Approve and authorise any major deviation from agreed project plans, consider Change requests and decide on which to accept/reject and where necessary report to the CFT programme Board.
- Ensure that risks and issues are tracked and mitigated as effectively as possible.
- Monitor the delivery of products to agreed time, cost and quality parameters and assign a RAG status.
- Make decisions on exception situations (including scope and requirements) beyond the authority of the HMCTS Service Owner, within the tolerances set by the Delivery Board.
- Provide any necessary guidance to the HMCTS Delivery Manager.
- Ensure that any events in the project or wider environment which may impact on the project are notified to the HMCTS Service Owner.

Project Documents

- The Supplier shall keep the Prioritised Requirements List, Resource Tracker and Implementation Plan under **review in accordance with the Delivery Board's instructions and ensure that they are maintained and updated on** a regular basis as may be necessary to reflect the then current state of the provision of the delivery of the **solution. Any reasonable changes or provisions to each version of the Prioritised Requirements List and** Implementation Plan shall be managed by the Delivery Board.

DISCOVERY PHASE

The Supplier shall undertake an initial phase of Discovery work across all In-Scope Courts and Tribunals to define and agree the Prioritised Requirements List (as more specifically defined below) and the Implementation Plan, in accordance with the Discovery Plan.

The Discovery tirneline, Activities and Deliverables
The proposed initial Discovery phase is for an estimated period of 10 weeks (5 two week Sprints). During the Discovery phase, the Supplier will undertake the following activities, and deliver the following key work products:

ACTIVITY	DESCRIPTION	DELIVERABLES
Project Kick-Off	The Parties key representatives will meet to get an overview of the project, and to agree the Project Charter.	Project Charter, to inclnde, the Terms of Reference, and the Project/Programme Governance Framework
Business Review Workshops	The Supplier will conduct functional requirements validation/fit analysis workshops with representatives from each of Jurisdictions. Where possible, these workshops will take place on location at the Jurisdictions. During these workshops, the Supplier will demonstrate the CE-File Service and/or the core C-Track solution suite, and discuss Annex 1 (High-Level Requirements) to validate the Supplier's understanding of Annex 1 and to agree with the Buyer a more detailed list of configuration **and customisations changes required to implement Annex** 1. During the workshops, the Supplier will validate **reporting and management information requirements in** addition to the functional requirements. This stage provides the Parties with a holistic view across the entire project to enable it to phase the overall programme in a prioritised way.	A Prioritised Requirements List (PRL) using MoSCoW prioritisation (Must, Should, Could, Won't)
Data Migration Analysis	During the Discovery phase, the Supplier will work with representatives from the relevant In-Scope Court and Tribunal, and subject matter experts, made available by the Buyer, who understand the data model schema and the technical architectnre and specifications of the legacy systems from which data will be migrated into the CE-File service. This will allow the Supplier to determine the specific requirements of the in-scope data migration work The Buyer will decide what data is to be migrated and will al!ree the process, format and timescales with the	Data Migration Design and Implementation Plan

	Supplier during the Discovery phase.	
Integration Analysis	The Supplier's understanding is that the Buyer will want the CE-File Service to integrate with, at least, the Gov.uk - Pay service and possibly the Gov.uk - Verify service; and other UK Government, or third-party services required by the Buyer to integrate with the CE-File **service** During the Discovery phase, the Supplier will work with representatives from HMCTS Digital Change team, the Mo) Digital Services, and Government Digital Services, as made available by the Buyer, to understand the technical **requirements for required integrations.**	Proposed Integration Design and Development Plan
Training Plan Analysis	During the Discovery phase, the Parties will meet to discuss the Training Plan further, and agree the specific training and collateral needs of the Buyer. For planning purposes the Supplier has assumed there are c.1,200 users connected with the In-Scope Courts and Tribunals as set out in the indicative volumes provided by the Buyer at Annex 2 to Schedule 1.	Training Plan

COURT and TRIBUNAL IMPLEMENTATIONS

The Supplier will deliver each Jurisdiction and Chamber within the In-Scope Courts and Tribunals in accordance with the following outline and the DSDM agile methodology; recognising that discovery (Feasibility and Foundations) will already have been conducted during the Discovery phase, and the complexity of configuration and customisation work required for each In-Scope Courts and Tribunals will be different. The Parties may decide to package In-Scope Courts and Tribunals together where their needs and dependencies are similar.

Exploration, Engineering and Deployment

The Supplier will undertake the delivery of the solution in a series of sprints to ensure decisions are taken in a timely way and keep progress on the project. The sprint approach will divide the project into smaller parts to provide demonstrable progress sooner to the In-Scope Courts and Tribunals.

- For each In-Scope Court and Tribunal, the development and implementation cycle will typically consist of six or seven sprints. The duration of each sprint consists normally of two or three weeks' development work
- Testing will be embedded into development
- At the end of each sprint, the Supplier will conduct a sprint review meeting with the Buyer's Service Manager to review the work completed during the sprint, seek approval to sign off the sprint, and finalise which requirements will be delivered in the next sprint
- The timing of the sprints is dependent on availability of Court and Tribunal resources as this is a collaborative **process.**

ACTIVITY	DESCRIPTION	WORK PRODUCT
Planning	Work with representatives of the relevant Court and Tribunal, made available by the Buyer to identify all of the configuration data (case events, etc) and all relevant artefacts for configuration (standard templates, seals etc) required to implement the jurisdiction onto the CE-File service, and identify specific reporting requirements Undertake legacy data mapping working to design the data migration scripts	Configuration Plan Data Migration Design and Plan
Configuration	Configure the CE-File service with all relevant configuration data and artefacts The configuration can be run in parallel with the Planning workstream when sufficient configuration items have been signed off by the Jurisdiction This workstream will be run in a series of sprints; each sprint following the sprint plan below.	Configured Solution
Development	Develop, build, test and implement any customised changes to the C-Track core product suite, and implement functional changes to the CE-File service Development will continue in parallel with the Configuration work following the same sprint plan, and review cycle Develop data migration scripts	Upgraded solution ready for UAT
User Sprint Testing	At the end of each sprint there will be a show and tell led by the Supplier's Business Analyst to demonstrate to users, the customised features and configuration agreed for delivery in the Sprint Users will be able to test these features and we will use this activity to gather feedback from users and the Buyer's Business Ambassador for the Court or Tribunal **regarding bugs, issues and to prioritise user stories for** the next sprint	
Deploy	After the final sprint for the Jurisdiction has been completed, the application will be released to the staging environment for integration testing, regression testing and performance testing. The final trial run of the data migration will be run in the secure data migration environment for sign off On sign off the Jurisdiction will be released with the rest of the Jurisdictions in the same tranche	Migrated Data

Test and Qp.ality Assunmce

The Supplier's testing methodology will use iterative build-test-release cycles during system development to meet a high level of quality assurance. Testing will be conducted in different test cycles and phases as follows:

- Unit Testing: Individual components tested in isolation by a Developer as they are implemented;
- System Testing: System testing is the process of combining application modules that have been tested through unit tests. This level of testing is performed once the various components of the application are working together, to ensure that the system functions correctly while performing the proposed business functions, without introducing unexpected errors. Any defects found are logged, assigned, fixed, and retested;
- **Integration Testing: Integration testing assures that workflow and communications between systems can be** performed seamlessly, for example, ensuring that the CMS communicates correctly with document management, e-filing, and external systems. Any defects found are logged, assigned, fixed, and retested; and
- User Acceptance Testing (with the Court or Tribunal's participation): When an early version (alpha) of the system is ready for review, the Court or Tribunal will perform user acceptance testing. The Court or Tribunal test team will use the fully-functioning system and the previously developed test plans to determine whether the system complies with the functional specifications.

Legacy System Data Migration

During this phase, the in-scope data migrations required for the In-Scope Courts and Tribunals will be developed and there will be an allowance in the Implementation Plan for up to three (3) trial runs of the migrations into the Secure Data Migration (SDM) Environment for the Buyer to check the data.

Data Migration Services

A data migration plan including which courts and tribunals are in scope will be agreed as part of the Discovery phase.

Assumption: The Supplier has assumed from the Buyer's indicative plan and High-Level Requirements that there are 10 **migrations in scope.**

The Supplier's data migration projects include the following in-scope and out of scope activities:

IN SCOPE	
Data Analysis	• Analyse Source data (any data which is not covered in Data Analysis exercise) during the discoverv phase
Mapping	• Map target tables with source tables by comparing existing application UI and C-Track application UI • Map source and target columns for each table • Map Document information (path, user access permissions, etc) from source data to CE-File database • Define logic to migrate source data to CE-File database • Document migration (move Documents from source file server to CE-File file server). Identify missing source data and map default data to target
Develop Scripts/ETL	• Generate migration scripts by implementing migration logic to migrate source data to CE-File Database • Execute the scripts on sample data
Data Validation/Testin	• Validate CE-File data (on the sample data) • Fix the issues (found after running scripts on real data) reported by the Buyer

Data Security	• The Supplier will only be responsible once the encrypted data has been signed over in to the custody of the Supplier. The Bu er is responsible for transferrin the data to the Supplier.

OUT OF SCOPE	
Data Quality	• Data correction (if any issues are found in source data during testing these will not be corrected by the Supplier but will be identified and passed back to the Buyer)

New Front-End Service Delivery

As part of the implementation project, it is anticipated that the Supplier will deliver a new front-end solution for the E-Filing and Public Access parts of the CE-File Service to enhance the accessibility and assisted digital aspects of the service. The Parties agree there will be a phased roll-out of the new front-end services as agreed in the Implementation Plan

4. TRAINING PROVISION

The Supplier will provide a senior, dedicated trainer to deliver blended training to users. This trainer will be supported by **an additional trainer.**

The trainers will create the digital training tools and manuals, facilitate WebEx (or Skype) training sessions and deliver face-to-face training on site at each of the In-Scope Courts and Tribunals. The Supplier will review and adapt the training plan alongside the Buyer's project team during the discovery phase to bring in suggestions from the Buyer's project team and consult with the stakeholders at each of the individual courts and tribunals. This phase will include finalising a **training sequence to mirror an agreed roll-out sequence, visits to each court and tribunal to assess the technology** available to support training, and training plans tailored to the circumstances of each different court and tribunal environment. The trainer will also utilise the skills and expertise of the established CE-File super user community within the Business and Property Court. Requirements and final pricing will be agreed during the Discovery phase.

Differences across each of the courts

The training will be customised to the unique needs of each Court and Tribunal depending on the configuration and functionality that has been set up for that Court or Tribunal. As staff in each Court and Tribunal are trained to use the system, they will become part of the trainer pool that can assist other Courts and Tribunals introducing case management for the first time. The technology available within each Court and Tribunal needs to be assessed by the Parties to facilitate **a successful training programme.**

Example course descriptions

Each course/module will be designed to cover all the necessary features and functions of CE-File. Depending on each configuration, some features and functions may not be enabled for a Court or Tribunal. The final list of features and functions configured and requiring training will be determined ahead of implementation.

Training Assumptions

The assumption is that all users have a reasonable level of computer literacy and are able to access the internet, view videos and able to access online WebEx training sessions both within the_ courts and tribunals, as well as remotely. The Supplier will work with the Buyer project team to further clarify requirements and build a jointly agreed training scope and schedule. The final scope and price to be agreed during the Discovery

28.

EXIT ACTMTIES AND TRANSITION

The Supplier will work with the Buyer to agree an exit and transition plan (the 'Exit Plan'), which will detail all data and technical transition activities to enable the Buyer to receive a copy of the data held at point of transfer in the CE-File Service. The data will be provided in a non-proprietary format such as CSV, XML,)SON etc. The structure of the data must be documented such that it can support the process of migration into an alternative product. At the end of Call-Off Contract, it is assumed that, once the Buyer is content all data has been provided, that all the data transferred (personal and otherwise) and the copies thereof will be destroyed and that the Supplier will certify to Buyer that it has done so. The **Buyer will have a right, upon reasonable notice, to audit, or seek alternative assurance, that the information/data had** been destroyed appropriately.

The Supplier should produce an outline Exit Plan (within the parameters set out above), agreed in principle with the Buyer no later than three (3) months after the final CE-File Service solution has been fully implemented. Critical activity and dates should be included that allow the Buyer to understand when key exit activities are anticipated to take place.

ANNEX 1 to SCHEDULE 1

HIGH LEVEL **REQIBREMENTS**

The following functional and non-functional requirements set out in Annex A- High Level Requirements shall apply to this Schedule 1:

Annex A - High Level Requirements

IN-SCOPE COURTS AND TRIBUNALS

The following Indicative Rollout Plan and Volumes were provided to the Supplier to provide an estimated cost of service as set out in this Call-Off Contract.

Indicative Rollout Plan and Volumes Fi

The Bill of Sale operates as a register of securities without case management by HMCTS. On the date of this Call Off Contract, Bill of Sale is agreed to be out of scope unless the Supplier provides a more affordable solution for providing this limited set of functionality. In the event an affordable solution is proposed by the Supplier and the Buyer wishes to bring this back in scope then any such change shall be agreed between the Parties in accordance with the Variation process.

ANNEX 3 to SCHEDULE 1

SERVICE LEVELS

1	**Priority** 1 An Incident which makes a critical function of the application(s)/Service inaccessible. No workaround exists.	Within 1 Service Hour from our receipt of an Incident ticket from Buyer's first or second line support provider using agreed ticketing system, Supplier will respond and confirm **commencement of** Incident resolution.	Supplier will prioritise resources to investigate the **root cause of an Incident** following receipt of a ticket, and work diligently to provide a fix and/or a workaround agreed with the Buyer (such agreement not to be unreasonably withheld) as soon as is reasonably practicable.	If an Incident is not resolved within 24 hours from our receipt of an Incident ticket from Buyer's first or second-line support provider, using agreed ticketing system, the Supplier shall confirm an agreed escalation plan to provide regular updates of progress, and **increased oversight from** Supplier's senior mana ement.
2	**Priority 2** Critical functionality degraded or unusable, having a **severe business** impact affecting multiple users. No **workaround exists.**	Within 4 Service Hours from our receipt of an Incident ticket from Buyer's first or **second line support** provider using agreed ticketing system, Supplier will respond **and confirm commencement of Incident resolution.**	Supplier will prioritise **resources to investigate the root cause of an Incident** following receipt of a ticket, and work diligently during **Service Hours to provide a** fix and/or a workaround agreed with the Buyer (such agreement not to be unreasonably withheld) as soon as is reasonably practicable.	If an Incident is not resolved within 5 Service Days from our receipt of an Incident ticket from **Buyer's first or second-line** support provider, using agreed ticketing system, the Supplier shall confirm an agreed escalation plan to provide regular updates of progress, and increased oversight from **Supplier's senior management.**
3	**Priority3** Non-critical function **or procedure,** unusable or hard to use having an operational impact. No workaround is available. Any Priority 2 Incident where an agreed workaround has been provided.	Within four Service Hours from our receipt of an Incident ticket from Buyer's first or second line support provider using agreed ticketing system, Supplier will respond and confirm **commencement of** Incident resolution.	Supplier will prioritise **resources to investigate the root cause of an Incident** following receipt of a ticket, and work during Service Hours to provide a fix and/or a workaround agreed with the Buyer (such agreement not to be unreasonably withheld) as soon as is reasonably practicable.	If an Incident is not resolved within 1 month from our receipt of an Iocident ticket from Buyer's first or second-line support provider, using agreed ticketing system, the Supplier shall confirm an agreed escalation plan to provide regular updates of progress, and increased oversight from Supplier's senior management.
4	Priority 4 Application or personal procedure unusable, where a **workaround is available or a repair**	During Support Hours, Supplier will respond within a reasonable period to Incident tickets from Buyer's first or second line	Supplier will deploy **resources to investigate the root cause of an Incident** following receipt of a ticket, and provide a fix and/or a workaround	If an Incident is not resolved within 1 quarter from our receipt of an Incident ticket from Buyer's first or second-line support provider, using agreed ticketing system, the Supplier

	is possible. All other incidents **that are not covered** by Priority 1, 2 & 3.	support provider using agreed ticketing system and confirm receipt of the Incident.	agreed with the Buyer (such agreement not to be unreasonably withheld) in **a manner prioritised with** the Buyer.	shall confirm an agreed escalation plan to provide regular updates of progress, and **increased oversight from Supplier's senior management.**

(a) Service Day - Monday to Friday other than public and bank holidays in England and Wales

(b) Service Hours - 07:00-18:00 in England and Wales on Service Days

AVAILABILITY

The CE-File Services will be available to the Buyer for at least the following percentages of the following periods:

- in relation to the C-Track Case Management System proposition, 99.9% of the time during Service Hours; and
- in relation to the C-Track E-Filing proposition, 99.5% of the time, 24 hours a day, 7 days a week.

In the event of the loss of any production hosting environment, the Supplier shall failover the Services to the disaster **recovery hosting environment, such that the Services are restored online within 2 Service Hours.**

In the event of the loss of any production hosting environment, data loss shall be restricted to the last 15 minutes of **transactional activity.**

A full back-up of the CE-File Services' databases shall be taken at least every twenty-four (24) hours and stored in a separate location; local incremental backups shall be taken every thirty (30) minutes.

PERFORMANCE

In its live configuration, the CE-File Service shall be capable of coping with a load that is 50% greater than the expected peak. During the peak hour, the back-end application is expected to deal with:

- 2000 online claim form submissions.

- 10000 case retrievals.

The CE-File Service must be configured in line with the law, regulations and the Authority's policies, standards and guidance including but not limited to Malware policy, patching policy, password standard, information handling, security. monitoring etc. The supplier must capture availability statistics for all servers directly associated with the application. Wherever possible monitoring statistics for publication to Authority should be captured at least every hour.

Availability, Performance and Service Level Exceptions

The Supplier will use all reasonable endeavours to achieve the Service Levels, however, the Buyer acknowledges and agrees that the Supplier shall not be responsible for any failure to meet the Service Levels caused by (whether in whole or in part):

- planned downtime of the CE-File Services
- **circumstances beyond Supplier's reasonable control, including but not limited to Force Majeure events, Internet connectivity failures, denial of service attacks and similar;**
- power, network or other IT infrastructure fault or failure which is under the control of the Buyer and/or its third party suppliers, including but not limited to such IT systems to which the CE-File Services are to interface with;

- failure and/or delay by the Buyer in performing a Buyer Responsibility, or Buyer Responsibilities;
- use of the CE-File Services by or on behalf of the Buyer in breach of this Call-Off Contract;
- use of the CE-File Services by or on behalf of the Buyer in excess of the Performance requirements set out below;
- deliberate misuse of the CE-File Services by or on behalf of the Buyer;
- unauthorised modification, repair and/or alteration of the CE-File Services by or on behalf of the Buyer without the consent of the Supplier; and/or
- the use of the CE-File Services for a purpose which it was not designed with reference to the description set out in this Call-Off Contract.

ANNEX 5 to Schedule 1

INDICATIVE DISCOVERY PLAN

[REDACTED]

[REDACTED]

[REDACTED]

Dependencies

The successful completion of the deliverables is dependent on the following:

Commitment from HMCTS to the milestone dates

Delivery ofrequested documentation on time

Availability of Buyer staff for meeting, review documents and sign off in line with the delivery plan

- Buyer to provide API details for integrations in advance of the Integration Workshops
- Buyer to provide the following before the Data Migration Workshops
    - Database Schema
    - Technical Specification of database documents containing business mapping to database fields
    - Number of records to be migrated
      Time period for data to be migrated
      Number of documents to be migrated (where applicable)

ANNEX 6 to SCHEDULE 1
TRAINING SERVICES

[REDACTED]

Schedule 2 - Call-Off Contract charges

1) All pricing in this Schedule 2 is stated exclusive of VAT.
2) The Supplier's rate card pricing for each of the G-Cloud Services are set out in Table 1 and Table 2.
3) The Supplier's charging assumptions for the provision of this G-Cloud Service is set out in Tables 3 to 8. These charges are based on the Supplier's estimates of delivering the High-Level Requirements (as defined in Annex 1 of Schedule 1) at the date of this Call-Off Contract, and the estimated case volumes for each In-Scope Courts and Tribunals (as set out in Annex 2 of Schedule 1) such Charges could be subject to change following the Discovery phase.

PRICE PER CASE FOR C-TRACK CMS SAAS AND C-TRACK E-FILING SAAS

[REDACTED]

Table 1

[REDACTED]

Discount
[REDACTED]

Transferred Cases

As a principle, the Parties agree that transferred cases should not attract more than one cost per case fee. The cost per case will be captured by the court or tribunal in which the action was started even if the case is immediately transferred out to another jurisdiction. If the case is given a new claim number as part of the transfer process it does not mean it will attract a new cost per case fee.

Cost per case fees are payable where there is some form of originating process i.e. in first instance courts or tribunal - a claim form or judicial review form. In Appellate jurisdiction, the originating process will either be the Permission to Appeal application or the full Appeal Application. Where both happen in the same jurisdiction the cost per case fee should only be paid once. Where Permission to Appeal is granted at the lower court or tribunal it does not attract a new cost per case charge but would, when the full Appeal is lodged at the Appellate Court or Tribunal.

Invoicing

As set out in the Order Form the Supplier will invoice monthly in arrears for the CE-File Services based on a monthly average forecast volume for the relevant Reporting Period, including for new Courts and tribunals deployed onto the CE-File Service. At the end of each quarter during the Reporting Period, the Parties will undertake a true up to verify the amount invoiced by the Supplier during the previous quarter aligns with the actual charges owed by the Buyer for the previous quarter, and will adjust future invoices accordingly.

SIFA RATE CARD

The Supplier has provided a high-level estimate, based on the following principle:

At the end of the Discovery phase, the Supplier will provide the Buyer with revised pricing for delivering the agreed Prioritised Requirements List in accordance with the agreed Implementation Plan and methodology described in Schedule 1 of this Call-Off Contract.

The Supplier will undertake a Discovery phase on a time and materials basis using the rates set out in the table below. At the end of the Discovery phase the Supplier will firm up costs for the agreed Prioritised Requirements List (based on MoSCoW with an agreed level of contingency) in accordance with the agreed Implementation Plan and methodology described in Schedule 1 of this Call Off Contract, and subject to an agreed set of assumptions and dependencies that will be set out in the Implementation Plan.

Table 2
[REDACTED]

The costs set out below in Tables 3 to 8 are provided by the Supplier on an indicative basis for undertaking the Implementation Services, and providing the Training Services, to change the CE-File Services to implement the High-Level Requirements and calculated using the rate card above and based on:

- the Supplier's knowledge of requirements which we have previously discussed with the Buyer's team at the Rolls Building;
- the Supplier's experience of, and the methodology used for, implementing the CE-File solution with the Business and Property Courts.

SUPPLIERS FORECAST COSTS

On boarding is the activity required, excluding system integration, prior to deployment into a Court or Tribunal. The elements covered are described in the extract from the Cost Model provided as part of the Supplier response to the GCloud Service.

The scope and timing of the deployment will be agreed as part of the discovery phase and may change during deployment e.g. if a lack of time to deliver within the required timescales requires scope to be reviewed.

Therefore, the costs set out in Tables 3 to 8 below are indicative.

Table 3 - On-boarding (Design and Configuration)

[REDACTED]

;Initiation, Design and Configumtion services *(incl. Discovety, Alpha, Beta stages when using en Agile approach)*	We have provided a breakdown of resource days and rates for the entire programme of work in Part F {Price Response)
Bills of Sale requirements ·Ability to record bills of sale transactions and generate Bill of Sale certificates	
8111s of Sale requirements 'Ability for external customers to create and pay for bins of sale on !line and be able to download bill of sale certificates	
Application Enhancements of current product. Product Change	Note, this excludes enhancement work for Bill of Sales requirement. We have provided a breakdown of resource days and rates *for* the entire programme of work in Part F (Price Response)
Planning ond Project Management	We have provided a breakdown of resource days and rates for the entire programme of work in Part F (Price Response)
Environments Setup end Management Supplier Testing (I.e. System. UAT. End lo End, Performance)	·ronments are alread o rational is is included within costs provided for nfiguration Services. and Enhancements have provided a breakdown of resource days programme of work in e
Service Desk 1st/2nd/3rd line Setup end system Integration	
Testing environments Testing envlronment Inslallation and Configuration Deployment release and hypercare for 2 weeks	ents are alread o rational enls are alread o rational n of resource days and rates for the gramme ofwork in Part F (Price

Table 4- On-boarding (System Integration)

System Integration is considered part of the on-boarding process to enable the E-Filing and CE-File to be successfully deployed into a Court or Tribunal. The elements covered are described in the extract from the Annex B - Cost Model - provided as part of the procurement process.

The Discovery phase will help inform what data will be migrated onto CE-File.

[REDACTED]

Plannlng and Project Management	
Environments Setup and Monagement Supplier Testin (i.e. System. End-to.End. Performance)	
Security Assurance and Accredl1ation services	,rs ment sure the security of requires third party addilional cost, s for.
Data Migration from current systems (cost each HMCTS :system separately, see tFR - CAP_003A)	O'M1 of resource days ogramme or work in

Table 5 - Training Provision

An agreed approach to training and how it is delivered will be agreed during the Discovery Phase and may be revised during the roll out to other Courts and Tribunals as a result of lessons learned and staff or professional user feedback. Therefore, these costs are indicative.

[REDACTED]

iImplementatlon training package (excluding Upper	Resource Costs.Assume a 1:20 for train the trainer= 56 to be trained
!Upper Tribunals Training Package	This is priced on our Option 1, as described in
jPrlnted material	• This is priced on our Option 1. as described in
!Trainglng Software Licences (Glance or Skype for Business)	
IHMCTS Standard HI h End Videos (2 Videos)	

Table 6 - Ongoing Charges (Service Management)

[REDACTED]

Table 7 - Offboarding Costs

[REDACTED]

Supplier Team - Migration ff-boarding	
Migration Equipment for Secure Data Transfer (purchase}	The price is for a 32IB NAS to transport the data securely. On current forecasts, we think his covers the expected volume of data with a 50% tolerance.

Additional Project Savings

Volume and other Savings

As set out in Annex B of the Supplier's tender response, the Supplier will apply 20% discount against the cost of implementation work (excluding Training Services) that will be phased as a single continuous programme.

Table 8

[REDACTED]

Part B - Terms and conditions

1. Call-Off Contract start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods ofup to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.62 (Data protection and disclosure)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Ftamework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

- **a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'**
- a reference to 'CCS' will be a reference to 'the Buyer'
- a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', **where** 'XX' is **the Framework Agreement clause number.**

2.4 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of **services**

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- **respond to any enquiries about the Services as soon as reasonably possible**
- complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or conttactors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ES! tool to assess whether the Supplier's engagement under the Call-Off Conttact is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material B_reach if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ES! tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ES! reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ES! reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when ntering into a Call-Off Contract they:

- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
- are confident that they can fulfil their obligations according to the Call-Off Contract terms
- have raised all due diligence questions before signing the Call-Off Contract
- have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business **continuity and disaster recovery plan is consistent with the Buyer's own plans.**

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will bepayable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working days ofreceipt of the returned invoice if it accepts the amendm,ents. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature ofG-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers' liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

- **a broker's verification of insurance**
- **receipts for the insurance premium**
- evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims **to insurers**
- promptly notify the insurers in writing of any relevant material fact under any insurances
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and **other evidence of insurance**

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

- premiums, which it will pay promptly
- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Act (DPA), or under incorporated Framework Agreement clauses 8.83 to 8.91. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary **business activities.**

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

- rights granted to the Buyer under this Call-Off Contract
- Supplier's performance of the Services
- use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

- modify the relevant part of the Services without reducing its functionality or performance
- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.7 Clause 11.5 will not apply if the IPR Claim is from:

- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
- other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material

Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

- comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data
- only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
- take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation and following **the Buyer's instructions**
- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

The Supplier must not remove any proprietary notices in the Buyer Data.

13.1 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's ana Buyer's security policy and all Buyer requirements in the Order Form.

13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

- the principles in the Security Policy Framework at ht1;jls:Uwww.gov.uk/governmentLpublications/securit;y-policy-framework and the Government Security Classification policy at ht1;jls:Uwww.gov.uk/governmentLpublications/government-securit;y-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at ht1;jls:Uwww.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information **Systems at httJ)s:ljwww.cpni.gov.uk/protection-sensitive-information-and-assets**
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at

s:

https:Uwww.ncsc.gov.uk/guidance/risk-management-collection

- **government best practice in the design and implementation of system components, including network** principles, security design principles for digital services and the secure email blueprint, available at htt;ps:Uwww.gov.uk/govemmentLpublications/technology-code of-practice/technology-code-of practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https:Uwww.ncsc.gov.uk/guidance/implementing-cloud-securit;y-principles

13.6 The Buyer will specify any security requirements for this project in the Order Form.

13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer **Data safe from unauthorised use or access, loss, destruction, theft or disclosure.**

13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in thls Call-Off Contract, the Order Form and the Framework **Agreement.**

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at https:Uwww.gov.uk/govemmentLpublications/technology-code-of practice/technology-code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If sofrware needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working

Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the **Services.**

16.2 The Supplier will use software and the most up-to-date antivirus definitions available from an industry-accepted **antivirus software seller to minimise the impact of Malicious Software.**

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

- Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

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

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

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start Date:

- an executed Guarantee in the form at Schedule 5
- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the **Guarantee**

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving the notice to the Supplier specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the

Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- anyfraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- an Insolvency Event of the other Party happens
- the **other Party ceases or threatens to cease to carry on the whole or any material part of its business**

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery ofsums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);l9 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)

- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by **implication is in force even if it Ends or expires**

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and **uncorrupted version in electronic form in the formats and on media agreed with the Buyer**
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 **Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.**

Mannerofdeliverv	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an error **message**

20.2 This clause.does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form {other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

21.4 The Supplier must ensure that the additional 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 of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- **there will be no adverse impact on service continuity**
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must 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 exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases 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 is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

- data (including Bnyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's **possession, power or control**
- other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with **immediate effect by written notice.**

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely forthe performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

- comply with any security requirements at the premises and not do anything to weaken the security of the **premises**
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving **the premises in a safe and clean condition.**

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person **which exists or is available otherwise.**

28. Environmental requrrements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start Date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes ofTUPE to the Services. For each person identified the Supplier must provide details of:

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- **salary, benefits and pension entitlements**
- employment status
- identity of employer
- **working arrangements**
- outstanding liabilities

- **sickness absence**
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

29.3 The Supplier warrants the accuracy of the information provided underthis TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to **communicate with and meet the affected employees or their representatives.**

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

- its failure to comply with the provisions of this clause
- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start Date in the form set out in Schedule 3.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

- work proactively and in good faith with each of the Buyer's contractors
- **co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's** ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations underthis Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional processing if permitted by Law).

33.2 The Supplier will provide all reasonable assistance to the Buyer to prepare any Data Protection Impact Assessment **before commencing any processing (including provision of detailed information and assessments in relation to** processing operations, risks and measures) and must notify the Buyer immediately ifit considers that the Buyer's **instructions infringe the Data Protection Legislation.**

33.3 The Supplier must have in place Protective Measures, which have been reviewed and approved by the Buyer as appropriate, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

33.4 The Supplier will ensure that the Supplier Personnel only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier Personnel with access to Personal Data, including by ensuring they:

i) are aware of and comply with the Supplier's obligations under this Clause;

ii) are subject to appropriate confidentiality undertakings with the Supplier or relevant Subprocessor

iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data.

33.5 The Supplier will not transfer Personal Data outside of the European Economic Area unless the prior written consent of the Buyer has been obtained and

i) the Buyer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Buyer and set out in Schedule 8 (International Data Transfer Agreement);

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

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

iv) the Supplier complies with any reasonable instructions notified to it in advance by the Buyer with respect to the processing of the Personal Data.

33.6 The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

33.7 The Supplier will notify the Buyer immediately if it receives any communication from a third party relating to the **Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide** the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation in. accordance with any timescales reasonably required by the Buyer.

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

i) the Buyer determines that the processing is not occasional;

ii) the Buyer 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; and

iii) the Buyer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

33.9 Before allowing any Subprocessor to process any Personal Data related to this Call-Off Contract, the Supplier must obtain the prior written consent of the Buyer, and shall remain fully liable for the acts and omissions of any Subprocessor.

33.10 The Buyer may amend this Call-Off Contract on not less than 30 Working Days' notice to the Supplier to ensure that it complies with any guidance issued by the Information Commissioner's Office.

33.11 Subject to clause 33.12, notify the Buyer immediately if it:

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

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

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

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

v) 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

vi) **becomes aware of a Data Loss Event.**

33.12 The Supplier's obligation to notify under clause 33.11 includes the provision of further information to the Buyer in phases as details become available.

33.13 The Supplier shall allow for audits of its Data Processing, activity by the Buyer or the Buyer's designated auditor.

33.14 The Supplier shall designate a data protection officer ifrequired under the GDPR.

33.15 This clause 33 applies during the Term and indefinitely after its expiry.

Schedule 3 - Collaboration agreement

The Collaboration agreement is available at https://www.gov.uk/g:uidance/g-cloud-templates-and-legal-documents

Schedule 4 - Alternative clauses

The Alternative clauses are available at https://www.gov.uk/g:uidance/g-cloud-templates-and-legal-documents

Schedule 5 - Guarantee

The Guarantee is available at https://www.gov.uk/g:uidance/g-cloud-templates-and-legal-documents

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, **documentation and processes** • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.

Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This Call-Off Contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement between the Buyer and any combination of the Supplier and **contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.**
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be **commercially sensitive.**
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: • **information about business, affairs, developments, trade secrets, know-**how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government **departments and particular bodies, persons, commissions or agencies carrying out** functions on its behalf.
Data Loss Event	Any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Call-Off Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach.
Data Protection Impact Assessment!	An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
Data Protection Legislation '	(i) the GDPR, the LED and any applicable national implementing Laws as amended **from time to time** (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy;

	(iiii) all applicable Law about the processing of personal data and privacy;
Data Protection Officer	Takes the meaning given in the GDPR.
Data Subject	Takes the meaning given 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.
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff {whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (h!;!;I!s:/Lwww.digitalmarketj2lace.service.g0v.uk/)
DPA2018	Data Protection Act 2018
Employment Regulations	The Transfer of Undertakings {Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information **Regulations or EIR**	The Environmental Information Regulations 2004 together with any guidance or **codes of practice issued by the Information Commissioner or relevant Government** department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14-digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: ht!;j2:/Ltools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure '	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any:

	• **acts, events or omissions beyond the reasonable control of the affected** Party • **riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare** • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557ix together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom oflnformation Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information **Commissioner or relevant Government department in relation to the legislation.**
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that 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 in a similar undertaking in the same or similar circumstances.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.

Indicative Test	ES! tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ES! tool.
Insolvency Event	Can be: • **a voluntary arrangement** • a winding-up petition • **the appointment of a receiver or administrator** • an unresolved statutory demand • a Schedule Al moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: • 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 names, designs, Know-How, trade secrets and other rights in Confidential Information • 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** • all other rights having equivalent or similar effect in any country or **jurisdiction**
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • **a service or a personal service company** • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPRC!aim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through **an Intermediary.**
IR35 Assessment	Assessment of employment status using the ES! tool to detertnine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Means 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 'oflaw,

	judgement in a relevant tribunal or directives or requirements with which the Supplier is bound to comply.
Law Enforcement Purposes	Means as it is defined in DPA 2018.
Loss	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 'Losses' will be interpreted accordingly.**
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed 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.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any **other single serious breach or persistent failure to perform as required under this** Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff **pensions: staff transfer from central government" issued in October 2013 as** amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries' legislation if assessed using the ESI tool.
Party	A Party to this Call-Off Contract.
Personal Data	Takes the meaning given in the GDPR
Personal Data Breach	Takes the meaning given in the GPDR
Processing	This has the meaning given to it under the Data Protection Act 1998 as amended but, for the purposes of this Call-Off Contract, it will include both manual and

	automatic processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the GDPR.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage **to:** • induce that person to perform improperly a relevant function or activity • **reward that person for improper performance of a relevant function or** activity • commit any offence: **0** under the Bribery Act 2010 0 **under legislation creating offences concerning Fraud** 0 **at common Law concerning Fraud** **0** **committing or attempting or conspiring to commit Fraud**
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
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 such measures adopted by it.
PSN or Public Services **Network**	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication **and share resources.**
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of **practice or otherwise, are entitled to investigate or influence the matters dealt with** in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.

Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https:ljwww.gov.uk/service-manuallagile-delivei;y,'spend-controls-check-if-iou-need-approval-to-spend-mone on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Sub-processor	Any third party appointed to process Personal Data on behalf of the Supplier related to this Call-Off Contract.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Personnel	**Means all directors, officers, employees, agents, consultants and contractors of the** Supplier and/or of any Sub-Contractor engaged in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	**A contract year.**

Schedule 7 - Processing, Personal Data and Data Subjects

1. The Supplier shall comply with any further written instructions with respect to processing by the Buyer.

2. Any such further instructions shall be incorporated into this Schedule.

Description·	Details
Subject matter of the processing	**This is a case management system to store and facilitate the storage and use of documents in relation to court and tribunal cases.**
Duration of the processing	The Application will be hold records in line with records Retention Policy **for each jurisdiction.** This currently varies across each jurisdiction from 3 to 20 years.
Nature and purposes of the processing	The purpose will include processing information and documents for the **purposes of case management of a court and tribunal case.** The Application shall hold:- • **Financial Information relevant to a case;** • **Commercial Information relevant to a case;** • HMCTS Statistics; and • HMCTS templates. **This information will include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.** **Th re will also be areas with restricted access to protect informatio on a need to know basis.**
Type of Personal Data	Personal information will be held within the case management system that will include name, • **Name;** • Address; • date of birth; • Employment details, relevant to the case; • telephone number; and • email address.

Categories of Data Subject	The Categories Subject are: • Members of the public that bring a case to the court or tribunal; and • Solicitors that act on behalf of a member of the public in bringing a case to court **or tribunal.**
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	Data will be retained in accordance with the HMCTS records Retention Policy for each jurisdiction. This currently varies across each jurisdiction from 3 to 20 years.

Schedule 8 - International Data Transfer Agreement

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third **countries which do not ensure an adequate level of data protection**

Name of the data exporting organisation: Ministry of Justice on behalf of HM Courts & Tribunal Services "Buyer"

Address: Director's Office, Royal Courts of Justice, Strand, London WC2A 2LL

[REDACTED]

Other information needed to identify the organisation:

[REDACTED]

And

Name of the data importing organisation: Thomson Reuters (Professional) UK Limited. "Supplier"

Address: Address: 5 Canada Square, Canary Wharf, London E14 5AQ
[REDACTED]

Other information needed to identify the organization:

[REDACTED]

each a "Party"; together "the Parties" under this Call-Off Contract.

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in ANNEX 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) ***'personal data: 'special categon·es of data: 'process/processing; 'controller: 'processor: 'data subject'*** **and** ***'supervisory authority'shall*** have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) *'the data exporter'means* the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'means* any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'means* the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) ***'technical and organisational security measures'*** **means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.**

Clause2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex 1 which forms an integral part of the Clauses.

Clause3

Third-party benefidarydause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to G), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation oflaw, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data

[1] Parties may reproduce definitions and meanings contained in Directive' 95/46/EC within this Clause if they considered it better for the contract to stand alone.

exporter by contract or by operation oflaw as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall **be limited to its own processing operations under the Clauses.**

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security **measures specified in Annex 2 to this contract;**

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all otherunlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause S(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the **suspension;**

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made **in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;**

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause5

Obligations of the data importer'

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter ofits inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the **transfer of data and/or terminate the contract;**

(c) that it has implemented the technical and organisational security measures specified in Annex 2 before processing the **personal data transferred;**

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement **investigation,**

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data **transferred;**

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, **unless the Clauses or contract contain commercial information, in which case it may remove such commercial** information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it lias previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they **constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and** prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic **society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anfr-money-laundering reporting requirements.**

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract ofby operation oflaw, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own **processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity** has assumed the entire legal obligations of the data exporter or data importer by contract or by operation oflaw, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek **remedies in accordance with other provisions of national or international law.**

Clause8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause9

Goveming Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely England & Wales

Clause JO

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses'. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as lald down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation oflaw. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph I shall be governed by the law of the Member State in which the data exporter is established, namely England and Wales.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 G), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parries agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Name (written out in full): [REDACTED]

Position: Director of the Royal Courts of Justice Group, London Region

Address: Director's Office, Royal Courts of Justice, Strand, London WC2A 2LL

Other information necessary in order for the contract to be binding (if any):

Signature... [REDACTED]

Name of the data importing organisation: Thomson Reuters (Professional) UK Limited. "Supplier"

Address: Address: 5 Canada Square, Canary Wharf, London E14 SAQ

[REDACTED]

Other information needed to identify the organisation:

(the data **importer)**

On behalf of the data importer:

Name (written out in full): [REDACTED]

Position: VP Market Development and Strategy

Address: 5 Canada Square, Canary Wharf, London E14 SAQ)

Other information necessary in order for the contract t e b" ding (if any):

Signature: [REDACTED]

ANNEX 1: INTERNATIONAL DATA TRANSFER AGREEMENT

1. Data exporter

The data exporteris (please specify briefly your activities relevant to the transfer):

The UK Ministry of)ustice on behalf of HM Courts & Tribunal Services who are responsible for the Courts and Tribunal services in the UK and maintain ownership of the CE-File production system data for the High Courts of Justice, the four chambers of the Upper Tribunal and the Employment Appeal Tribunal in England & Wales. This Order Form covers the exporting of data from the following High Courts and Tribunal locations where the CE-File Service is installed or planned for installation.

- Royal Courts of Justice, Fetter Lane, London, EC4A lNL
- Rolls Building, Queens Bench and Upper Tribunal chambers for Administrative Appeals, Tax and Land, Strand, London, WC2A 2LL
- Upper Tribunals in Field House, 15-25 Breams Buildings, London EC4A lDZ
- Employment Appeals Tribunal, 2nd Floor, Fleetbank House, 2-6 Salisbury Square, London EC4Y SAE
- **District registries and local administrative offices**

Note:

- Field and Fleetbank House based teams may move to the other London Offices.
- Due to the nature of the Buyer's Reform programme and the size of change happening in the organisation, the locations set out here may not remain the same but the number of jurisdictions being delivered will not change.

2. Data importer

The data importer is (please specify brieflyactivities relevant to the transfer):

Thomson Reuters Professional UK Ltd who are providing the CE-File Service to the High Courts of)ustice's, listed **under paragraph 1, for the management of documents and court case management data.**

There are two scenarios where the Supplier's offshore resources might be required to work with data directly from the CE-File production system, potentially giving them access to personal data (as defined under the Data Protection Act 1998), outside of the European Union.

(a) Scenario 1 - As a result of an Incident Ticket or Service Request raised by HMCTS
Off-shored resource may be required to check the status or comparison of the database, for example the number of open cases in the system with the expected number; or to check specific data (including personal data) in the production database.

(b) Scenario 2: During a release window
Off-shored resources may be required to check the status of the upgrade for example how many records have been migrated to particular tables.

As a result of the above scenario and on occasions, there might be a requirement for offshore resource to access personal data during a release window, for example if there is a problem with an individual's data which is **preventing a successful release.**

3. Data subjects

The personal data transferred concern the following categories of individuals:

All parties to the case i.e. defendants, claimants, applications, judges and court staff.

4. Categories of data

The personal data transferred concern the following categories of data:

Court case scheduling information, court case data, names and addresses of parties to the case, date of birth of parties to the **case, bank account details, names of organisations and their addresses**

5. Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Potentially any sensitive data included in the court case data including possible information about political opinions, sexual life, health, religous or similar beliefs, trade union or workers group affiliations, ethnicity or nationality or criminal **convictions or proceedings.**

6. Processing operations

The personal data transferred will be subject to the following basic processing activities inputting, storing, downloading and printing data

Name of the data exporting organisation: Ministry of Justice on behalf of HM Courts & Tribunal Services "Buyer"

Address: Director's Office, Royal Courts of Justice, Strand, London WC2A 2LL

[REDACTED]

Other information needed to identify the organisation:

[REDACTED]

And

Name of the data importing organisation: Thomson Reuters (Professional) UK Limited. "Supplier"

Address: Address: 5 Canada Square, Canary Wharf, London E14 5AQ

[REDACTED]

Other information needed to identify the organisation:

[REDACTED]

each a "Party"; together "the Parties" under this Call-Off Contract.

ANNEX2: CYBER SECURITY AND INFORMATION ASSURANCE REQUIREMENTS

1. SECURITY CLASSIFICATION & INFORMATION HANDLING

1.1. The Supplier and any 3" party suppliers shall support the Buyer's requirement to remain compliant with Her Majesty's Government (HMG) Security Policy Framework (SPF) and principles, obligations and policy priorities in accordance with the Cabinet Office website htq.s://www.gov.uk/govemment/collections/government-security and may be modified from time to time.

1.2. The information processed and stored *in* delivering the services described by this Order Form for all Parties *in* this contract, is classified under the Government Security Classifications scheme as OFFICIAL. Some of it may be OFFICIAL-SENSITIVE. The Supplier providing the services under this Order Form shall ensure that they and their delivery partners and wider supply chain apply at least the minimum security controls required for OFFICIAL information as described *in* Cabinet Office guidance detailed htq.s://www.gov.uk/govemment/uploads/system/uploads/attachment data/file/251480/Govemment-Security-Classifications-April 2014.pdf and as updated from time to time. The Supplier shall specifically consider paragraph 13 et seq. and the Technical Controls Summary for OFFICIAL at paragraph 41 for an overview of the security requirements applicable to this Order Form.

1.3. The Supplier must at all times ensure that the level of cyber security and information assurance is maintained to protect the confidentiality, integrity, and availability of information assets across all aspects of the service and **provide acceptable levels of risk management and /or risk acceptance so that the Buyer can maintain assurance** and accreditation as required by HMG guidance.

1.4. The Cyber Essentials Scheme (as detailed in paragraph 2.0), the Cloud Security Principles (as detailed *in* paragraph 3.0), and the security controls required for OFFICIAL information all complement each other with the aim of achieving sound commercial standards of security *in* relation to IT and information handling.

2. CYBER ESSENTIALS SCHEME

2.1. The Supplier shall demonstrate by the start date of the contract (or at a later date agreed by the Buyer) that they meet the technical requirements prescribed by Cyber Essentials scheme. This *is in* order to further reduce the levels of cyber security risks *in* their supply chains.

2.1.1. The Cyber Essentials Scheme and the related, published, Assurance Framework both indicate that there are two levels of protection *in* dealing with cyber security risks. These include a more basic level of assurance which is known as Cyber Essentials and a more advanced level of assurance known as "Cyber Essentials Plus". Details of the scheme are available at and may be updated from time to time:

https://www.cyberstreetwise.com/cyberessentials

3. CLOUD SECURITY PRINCIPLES

3.1. The Supplier shall also assurance responses to the HMG Cloud Security Guidance and the Cloud Security Principles as a source of security guidance and requirements as required and as detailed on https://www.ncsc.gov.uk/guidance/cloud-security-collection and as updated from time to time.

4. SPECIFIC REQUIREMENTS FOR CYBER ASSURANCE AND ACCREDITATION

4.1. The Supplier shall adhere to the following requirements of the assurance and accreditation of IT solution which supports the CE-File Service:

4.1.1. Security and Information Assurance: Procedural and Policy controls

4.1.1.1. The Supplier shall develop, implement, operate, maintain and continuously improve an Information Security Management System (ISMS). The ISMS must be aligned to ISO 27001:2013 and must be reviewed/ tested and periodically updated, at least annually, subject to agreement with the Buyer or when there is a significant change to the solution. The scope must cover any third-party suppliers.

4.1.1.2. The CE-File Service must comply with current legislation, and relevant HMG security standards.

4.1.1.3. **The Supplier must demonstrate procedures for the secure destruction and decommissioning of assets.**

4.1.1.4. The Supplier must, if requested, provide sufficient design documentation detailing the security architecture of **their information system and data transfer mechanism to support the accreditor's assurance that the service is** appropriate managed and secure, and complies with all specified security requirements.

4.1.1.5. The CE-File Service will be assured for handling Information classified as OFFICIAL (including OFFICIAL-SENSITIVE) and be subject to accreditation to HMG standards and meet the standards required for security controls for OFFICIAL information in accordance with the HMG Security Policy Framework, and consistent with HMG Security Policy, Standards and Guidance.

4.1.1.6. The CE-File Service will securely store and process all data recorded on the service to comply with HMG Security Policy, Standards and Guidance.

4.1.1.7. Where there are aspects of data aggregation, additional security controls may be required above the level of the HMG Baseline in accordance with HMG Security Policy, Standards and Guidance.

4.1.1.8. The Supplier must appoint an ICT system manager or security manager, who is responsible for the provision of technical, personnel, process and physical security aspects for the service.

4.1.1.9. The CE-File Service must comply with current legislation, relevant HMG security standards and the Buyer's security policies.

4.1.1.10. The CE-File Service must demonstrate procedures for reporting and responding to security incidents comply with **arrangements for reporting security incidents to the Buyer.**

4.1.1.11. The CE-File Service must demonstrate procedures for secure destruction and decommissioning of assets.

4.1.1.12. Any changes to the service must be made via the Variation process set out in Clause 32 of Part B, Terms and **Conditions.**

4.1.2. Security and Information Assurance: Physical and Environmental Controls

4.1.2.1. The Supplier shall ensure the CE-File solution is protected by appropriate people, process, technology and physical security controls as part of a 'defence-in-depth' approach.

4.1.2.2. The Supplier shall ensure the CE-File solution securely identifies and authenticate users before allowing them to **access the solution.**

4.1.2.3. The Supplier shall ensure where there are aspects of data aggregation, they adopt any necessary additional controls if required above the level of the HMG Baseline Controls in accordance with HMG Security Policy, Standards and Guidance subject to agreement with the Buyer's accreditor.

4.1.2.4. The Supplier shall ensure that any electronic transfer of data:

4.1.2.4.1. Protects the confidentiality of the data during transfer through encryption suitable for the classification of the **data;**

4.1.2.4.2. Maintains the integrity of the data during both transfer and loading into the receiving solution through suitable technical controls for the impact level of the data;

4.1.2.4.3. Prevents repudiation of receipt through accounting and auditing.

4.1.2.5. The Supplier shall ensure that all solution information assets and supporting utilities provide appropriate physical **protection from internal, external and environment threats commensurate with the Buyer's business value of the** assets and aggregation where appropriate.

4.1.2.6. The Supplier shall ensure that all physical components of the solution must be kept in secure accommodation which conforms to HMG Security Policy, Standards and Guidance aod which can be independently audited and approved by the Buyer or its authorised representative.

4.1.2.7. The Supplier shall ensure all handling of physical media containing Security Classified (OFFICIAL) data must be done in accordaoce with HMG (Security Policy Framework) and Communications-Electronics Security Group (CESG) standards aod guidaoce or equivalent good commercial practice.

4.1.3. Security aod Information Assuraoce: Technical Controls

4.1.3.1. The Supplier shall ensure the CE-File Service solution must provide network controls to authenticate internal **and external users prior to communicating to prevent unauthorised users gaining access to services and** information.

4.1.3.2. The Supplier shall ensure that the import and export of data from the solution must be strictly controlled aod recorded **/** audited.

4.1.3.3. The Supplier shall ensure the CE-File Service solution must enforce the principle of 'least privilege' and only **grant users the minimum necessary permission to access information/ access the service.**

4.1.3.4. The Supplier shall ensure the CE-File Service will enforce robust role-based access control mechanisms to prevent unauthorised access to data.

4.1.3.5. The Supplier shall ensure the CE-File Service solution must implement effective and legitimate monitoring of the service in accordance with HMG staodards, applying CESG Good Practice Guide (GPG) 13 - Protective Monitoring where applicable and as required by the Buyer's accreditor.

4.1.3.6. The Supplier shall, where appropriate and as required by the Buyer's accreditor, ensure that the service functions **in accordance with current best practice for Protecting External Connections to the Internet.**

4.1.3.7. The Supplier shall ensure that the solution functions in accordance with current best practice for Protection from Malicious Code.

4.1.3.8. The Supplier shall ensure that all components of the solution are patched in line with accepted commercial good practice; the approach to this must be documented in a patch management policy agreed with the Buyer.

4.1.3.9. The Supplier shall ensure that an IT Health Check is conducted on the CE-File Service on an annual basis by an independent CHECK qualified compaoy or internally to an equivalent staodard, if aod as required by the accreditor and subject to agreement on its scope; it being understood that if the Buyer requires an independent CHECK qualified company to carty out the IT Health Check, the Buyer shall reimburse the Supplier for the costs of such independent CHECK qualified company. The Buyer shall maintain the right to see the reports·and remediation of any external or internal testing completed.

4.1.3.10. The Supplier shall ensure that technical vulnerabilities are managed effectively and must be recorded on the solution risk register and tracked through the Risk Treatment Plan as a product of the accreditation process

4.1.3.11. The Supplier shall ensure that the CE-File Service functionality includes the automatic logging out of users out of **the service if an account/ session is inactive for more than 15 minutes.**

4.1.3.12. The Supplier must provide sufficient design documentation detailing the security architecture of their information system aod data transfer mechanism to support the Buyer's assurance that the service is appropriate **and secure.**

4.1.3.13. The Supplier shall provide internal processing controls between security domains/tiers where applicable and as required by the Buyer's accreditor, to prevent a higher domain/tier exporting unauthorised data to a lower domain/tier without approved controls.

4.1.3.14. The Supplier shall ensure that any sensitive personal data and any OFFICIAL-SENSITIVE data must be encrypted **in transit and wh n at rest if stored away from the Supplier's controlled environmfnt.**

4.1.3.15. The Supplier shall ensure that the service provides controls to securely manage (store and propagate) all **cryptographic keys to prevent malicious entities and services gaining access to them, in line with the Buyer's** Cryptographic Policy (if stipulated by the Buyer's accreditor) or commercial best practice stipulated in ISO 27001:2013.

4.1.4. Security and Information Assurance: Personnel Controls

4.1.4.1. The Supplier shall ensure that all Supplier personnel that have logical or physical access to the service or Buyer Data are security cleared to a minimum of "Security Check National Security Vetting" or subject to appropriate clearance of outside the UK.

4.1.4.1.1. Personnel that do not have access must be cleared to the Baseline Physical Security Standard (BPSS) or to a recognised equivalent standard (note: BS 7858 would meet the requirement), or the Supplier must provide evidence that they have controls to prevent these personnel from gaining access. This requirement is without prejudice to any overarching vetting requirements set out in the Call-Off Contract.

4.1.4.1.2. The Supplier shall ensure that any delivery partners or third-party suppliers are subject to the same security **arrangements and meet the same personnel controls and security requirements that are expected of the Supplier.**

4.1.4.1.3. **Both Parties must ensure procedures are in place to ensure all Supplier Personnel who have access to data are** aware of their responsibilities when handling the data and the solution used to process it.

4.1.4.1.4. The Supplier shall ensure that the CE-File Service !CT manager is a UK national.

4.1.4.1.5. The Supplier shall support the Buyer's obligations to comply with any current HMG policy regarding the use of **off-shore resources, assessing and managing any additional security risks associated with the storage, processing**or transmission ofinformation offshore, typically by an offshore provider or sub-contractor (which may includethe use of 'landed resources'), taking account of EU requirements to confirm the 'adequacy' of legislated protection of personal information in the country(ies) where storage/ processing occurs. No element of the CE-File Service may be 'off-shored' without the express written permission of the Buyer.

4.1.4.1.6. The Supplier shall ensure that effective training and awareness is in place to ensure that the provider's personnel and those of any sub-contractor are aware of and apply all information security requirements relating to their role(s).

ANNEX 3: PROCESS FOR MANAGING DATA TRANSFER WITH OFFSHORE RESOURCE

Both Parties shall ensure they adhere to the process detailed below when managing personal and sensitive personal information (as defined by the Data Protection Act 1998 and General Data Protection Regulation 2018).

The Buyer may require this process to be updated from time to time to comply with HMG Off-shoring policy {as detailed in Annex 2) and the Data Protection Act 1998 and General Data Protection Regulation 2018 principles.

The Supplier shall ensure appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The Supplier shall ensure personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in **relation to the processing of personal data.**

There are two scenarios where the Supplier's offshore resources might be required to work with data directly from the CE-File production system, potentially giving them access to personal data (as defined under the Data Protection Act 1998), outside of the European Union.

(a) Scenario 1 - As a result of an Incident Ticket or Service Request raised by the Buyer
Off-shored resource may be required to check the status or comparison of the database, for example the number of open cases in the system with the expected number; or to check specific data (including personal data) in the production database.

(b) Scenario 2: During a release window
Off-shored resources may be required to check the status of the upgrade for example how many records have been migrated to particular tables.

As a result of the above scenario and on occasions, there might be a requirement for offshore resource to access personal data during a release window, for example if there is a problem with an individual's data which is preventing a successful release.

Buyer Responsible Person: As delegated by the Information Asset Owner on a day to day basis e.g. Senior Operations Manager, Rolls Building

Process for Scenario 1: Incident Ticket/Service Request

Step	Step Description	Responsible
1	Incident ticket is raised either by: • Buyer via their Helpdesk provider; or • Directly by Supplier system monitoring.	Buyer/Supplier
2	All activities to resolve the incident ticket are tracked within SM9 {the Supplier service management tool). All are linked to change requests invoked to resolve the ticket.	Supplier
3	If Supplier believes they need to query tables containing personal information {as defined by the Data Protection Act 1998), a request for authorization must be sent by the Supplier Service Manager (or nominated deputy) to the Buyer Responsible Person for approval.	Supplier

4	The Buyer's Responsible Person responds with authorisation to proceed via e-mail.	Buyer
5	Any data sent back to the Buyer by the Supplier must be presented in a password protected document; the password being sent separately either by e-mail or SMS.	Supplier
6	Once the incident is agreed as resolved, authorization to access that data will be revoked by default upon closure of the incident ticket.	Buyer/Supplier

All activity on the database shall be logged and all Supplier support staff are required to access the production environment via a jump server for auditing purposes.

Process for Scenario 2: During a Release Window

Step	Step Description	Responsible
1	The Supplier raise a Buyer Change Request Form (see below)	Supplier
2	The Buyer to obtain JSCAB approval to proceed with the release.	Buyer
3	The Buyer to relay JSCAB approval to the Supplier.	Buyer
4	All Supplier releases are tracked via change requests in SM9, which clearly specifies the start and finish times of the release window. Between these times Supplier will be authorized to query the database to ensure that the release scripts have run successfully and that migrations have completed successfully.	Supplier
5	If **there are issues with the release where there is a requirement to access personal data (as** defined by the Data Protection Act 1998), a request by e-mail will be made to the Buyer Responsible Person for the release, informing them of the personal data (as defined by the Data Protection Act 1998) they need to access.	Supplier
6	Buyer Responsible Person responds with authorisation to proceed via e-mail.	Buyer
7	Data sent back to Buyer by the Supplier must be presented in a password protected document; the password being sent separately either by e-mail or SMS.	Supplier
8	Once the release has been signed off by the Buyer Responsible Person, authorization to access that data will be revoked by default.	Buyer/Supplier

In addition to the two process scenarios detailed above, a Privacy Impact Assessment (PIA) screening and risk assessment shall be carried out under the co-ordination of the Buyer's Lead Accreditor.

Schedule 9 - Operational Working Agreement

1. The Operational Working Agreement ("OWA") is a living document that defines how the hand-off process will work between l" Line Support, the Supplier, Users, and the Buyer during the term of this Call-Off Agreement. The OWA reflects the current working practices of the Buyer and the Supplier. Both parties acknowledge and accept that the Supplier was providing similar services under contract CON_13771 31/03/2018 and that parties need to update the working practices set out in the OWA, during the Discovery phase. All mutually agreed amendments to the OWA **will be in writing and in accordance with the Variation process.**

CE-File OWA V3 01
100216.doc

Schedule 10 Buyer change request form

The Buyer's Change Request Form is produced by the Buyer and may be subject to change during the term of this Call-Off Agreement. It acts as an aid to decision making and governance for any change to a live application service by seeking **information on a range of subjects e.g. an overview of the change, impact and risk analysis, testing and resources.**

MoJ Joint Services
CAB Exarrple RFC Fol