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

**Order Form** 

Call-Off Reference:	PR 2023 070
Call-Off Title:	FCT Discovery and Phased Delivery Digital Capability
Call-Off Contract Description:	The Crown Prosecution Service (CPS) is undergoing a significant amount of transformational change as well as managing a large portfolio of change within its mission critical legacy systems. The work under this procurement will be to support the Digital and Information Directorate (DID) Future Casework Tools Programme providing expertise to deliver Digital capability for Discovery and phased Delivery development.
	This initiative is about organising case material, ensuring there is a high standard of quality in the data fields that CPS control i.e., labels, filenames, format etc. of material. Material should be made easily understandable and clear for user groups.
	The quality of data fields that CPS does not control e.g., the quality of witness statements by an Investigation Authority is not included.
	Addressing bundling errors because case material is unorganised or not maintained properly on the system is included.
	Problem Statement
	Case material is not presented with document management features, (effective search functions, categorisation) on the system making it difficult to review, delaying case progression milestones (charging decision, serving of material, case reviews.)
The Buyer:	Crown Prosecution Services
Buyer Address:	102 Petty France London SW1H 9EA

The Supplier:	Farsight Consulting Limited
Supplier Address:	Units 3.03-3.05, Canterbury Court, 1-3 Brix- ton Road, LONDON SW9 6DE
Registration Number:	7215255
DUNS Number:	216680896
SID4GOV ID:	Not applicable

#### **Applicable Framework Contract**

This Order Form is for the provision of the Call-Off Deliverables and dated 08/09/23.

It's issued under the Framework Contract with the reference number RM1043.8 for the provision of Digital Outcomes Deliverables.

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

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

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

#### Call-Off Lot

Digital Outcomes and Specialist (DOS) 6 - Lot 1 Digital Outcomes

#### **Call-Off Incorporated Terms**

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

- 1 This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
- 2 Joint Schedule 1 (Definitions) RM1043.8
- 3 Framework Special Terms
- 4 The following Schedules in equal order of precedence:
  - Joint Schedules for RM1043.8
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)
    - o Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data) RM1043.8

- Call-Off Schedules for RM1043.8r
  - Call-Off Schedule 1 (Transparency Reports)
  - Call-Off Schedule 3 (Continuous Improvement)
  - o Call-Off Schedule 5 (Pricing Details and Expenses Policy)
  - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)
  - o Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 9 (Security)
  - o Call-Off Schedule 15 (Call-Off Contract Management)
  - Call-Off Schedule 18 (Background Checks)
  - Call-Off Schedule 20 (Call-Off Specification)
  - Call-Off Schedule 25 (Ethical Walls Agreement)
  - o Call-Off Schedule 26 (Cyber Essentials Scheme)
- 5 CCS Core Terms (version 3.0.11)
- 6 Joint Schedule 5 (Corporate Social Responsibility) RM1043.8
- 7 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

#### **Call-Off Special Terms**

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

N/A

Call-Off Start Date:	25 <sup>th</sup> September 2023
Call-Off Expiry Date:	24 <sup>th</sup> March 2024
Call-Off Initial Period:	6 Months
Call-Off Optional Extension Period:	Up to 3 months
Minimum Notice Period for Extensions:	30 days
Call-Off Contract Value:	Up to £750k net
	(900k inclusive of VAT)
	Please note that CPS are not obliged to spend the full contract value.

# **Call-Off Deliverables**

Option B: See details in Call-Off Schedule 20 (Call-Off Specification)

# Warranty Period

N/A

# **Buyer's Standards**

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

https://www.gov.uk/government/publications/technology-code-of-practice/technologycode-of-practice

#### https://www.gov.uk/service-manual/service-standard

#### **Cyber Essentials Scheme**

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

#### **Maximum Liability**

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **125% of the** Estimated Charges in the first 12 months of the Contract (£186,712.50k).

#### **Call-Off Charges**

1 Fixed Price (as per each SOW).

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) and the Supplier shall, under each SOW, charge the Buyer a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

All changes to the Charges must use procedures that are equivalent to those in Paragraph 4 in Framework Schedule 3 (Framework Prices).

#### **Reimbursable Expenses**

It is anticipated that the supplier will be remote working, however the below T&S policy shall apply if staff are requested to travel.

- See appendix 2 of the work order

# **Payment Method**

The payment method for this contract shall be via Purchase Order.

The Customer shall make payments to the Supplier within thirty (30) days of receipt of a Valid Invoice, submitted in accordance with Call-Off Schedule 5 (Pricing Details).

#### **Buyer's Invoice Address**

#### Crown Prosecution Service Invoice Team



#### Buyer's Authorised Representative

Name	
Role	Head of Digital Case Management Programmes
Email	
Address	102 Petty France London
	SW1H 9EA

# **Buyer's Environmental Policy**

- See appendix 3 of the work order.

#### **Buyer's Security Policy**

- See appendix 4 of the work order.

# Supplier's Authorised Representative

Name	
Role	Managing Director
Phone	
Email address	
Address	Units 3.03-3.05, Canterbury Court, 1-3 Brixton Road, LONDON SW9 6DE

# Supplier's Contract Manager

Name	
Role	Head of Service Delivery
Phone	
Email address	
Address	Units 3.03-3.05, Canterbury Court, 1-3 Brixton Road, LONDON SW9 6DE

# **Progress Report Frequency**

Sprint 1 – supplier to produce the Delivery Plan

End of each sprint - supplier to produce a sprint report

End of Discovery – supplier to produce a Discovery report

CPS will produce highlight reports for a monthly scrum of scrums and the supplier will be required to complete a single highlight slide.

# **Progress Meeting Frequency**

The supplier shall attend and participate in the following.

- Agile ceremonies
- Daily stand ups
- Fortnightly Sprint Planning and Sprint Retros
- Fortnightly Show and Tells
- Monthly Scrum of Scrums
- Stakeholder meetings at the end of discovery.

#### Farsight Consultancy Ltd Key Staff

Name	
Role	Head of Service Delivery
Phone	
Email address	
	Units 3.03-3.05, Canterbury Court, 1-3 Brixton Road, LONDON SW9 6DE

#### Key Subcontractor(s)

Version 1 are a delivery partner supporting and providing resource to the Farsight team.

#### **Commercially Sensitive Information**

Supplier rate card and bid response.

#### **Balanced Scorecard**

N/A

#### Material KPIs

Deliverables and Milestones will be documented and agreed between both parties though each Statement of Work.

#### Service Credits

N/A

# **Additional Insurances**

N/A

# Guarantee

N/A

# **Social Value Commitment**

Social value commitment shall be provided separately, within one month of the start of the contract. The social value commitment will be reviewed as the contract progresses.

#### Statement of Works

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

#### For and on behalf of the Supplier:

Signature	
Name	
Role	Managing Director
Date	12 September 2023

#### For and on behalf of the Buyer:

Signature	
Name	

Role	Head of Commercial Digital - CPS
Date	25th September 2023

# Appendix 1

The Statement of Work to be agreed between both parties.

#### Appendix 2 – T&S Expenses

Rates of Travel and Subsistence as at 01/04/18 Subsistence- official business travel

Day Subsistence Rate more than 5 hoursup to	£4.50
more than 10 hoursup to	£9.75
more than 12 hoursup to	£13.55

Day Subsistence reimburses additional necessary expense incurred whilst more than 5 miles away from the permanent station.

All claims must be fully supported by receipts. In exceptional circumstances i.e. loss of ticket etc. explanations should be given for non- receipt.

#### **Overnight Subsistence**

Hotel Rates London and Metropoli- tan Areas of Birmingham, Man- chester, Leeds, Liverpool, Newcas- tle and York up to	£95.00
Elsewhereup to	£65.00

#### Personal incidental expenses

No more than £5- receipts for appropriate expenditure must be provided.

Overnight stay with family or friends or second home £25

(Staff choosing to stay with family or friends, or second home, cannot claim subsistence or Personal Incidental Expenses)

#### Travel

This should be the most cost-effective journey (taking into account travel time costs, car park fees, urgency, and whether public transport is a viable option. If a member of staff chooses to use their own vehicle when public transport is a viable option, their claim will be limited to Public Transport costs or Public Transport Rate mileage if this is less. Journeys should be agreed with line management before commencing).

Rail, Tubes, Buses and Taxis	Actuals supported by receipts
Private Motor Vehicle (with appropriate insurance):	
Business Rate per mile up to & including 10,000 miles *applies from 6th April 2011	*45p
Business Rate per mile over 10,000 miles	25р
Public Transport Rate (with appropriate insurance) per mile:	25р
Passenger Rate:	
1st passenger per mile	5р
2nd passenger per mile	2р

CPS Contract Car per mile	6.8p
<b>Car Park Fees</b> (Car park fees will only be paid if line man- agement have approved the journey to be made by private vehicle)	Actuals (supported by receipts)
Motorcycles (with appropriate insurance) Flat rate of	24p
Pedal cycles	20p

# **Appendix 3 Environment and Sustainability Policy**

1.1 The Customer and the Supplier shall be committed to promoting the conservation and improvement of the environment. The Customer policy on sustainable procurements:

1.1.1 to comply with environmental legislation and regulatory requirements;

1.1.2 to promote environmental awareness amongst suppliers and Suppliers;

1.1.3 to buy less environmentally damaging products and services;

1.1.4 to consider environmental factors when making procurement decisions; and

1.1.5 to develop awareness of environmental issues within the Customer organisation.

1.2 The Supplier must support this policy and apply similar policies within its own business. The Supplier shall as a matter of policy both recycle and use recycled products where possible and feasible to do so, and encourage environmentally sensitive attitudes in its personnel.

#### **Development of Products**

2.1 The Supplier shall contribute to sustainable development by developing, producing, and offering products and services with excellent environmental performance that shall enable the Customer to minimise their environmental impact. This means that the Supplier shall:

2.1.1 develop staff and sub Suppliers awareness of environmental issues to the level where consideration of environmental impacts becomes a natural part of daily work driving continual improvement and pollution prevention;

2.1.2 use lifecycle techniques as a means for determining significant environmental impacts and as a basis for actively communicating and continuously improving the environmental performance of their processes, products and services;

2.1.3 implement and maintain certified environmental management systems in any of its premises and operate a corporate-wide Environmental Management System that covers all of its operations;

2.1.4 meet or exceed legal and other requirements to protect the environment;

2.1.5 use design for the environment to introduce environmentally improved processes, products and services;

2.1.6 adopt a proactive approach to the supply-chain in order to ensure environmental control of the inputs to its products and processes;

2.1.7 actively communicate about the environmental work to internal as well as external stakeholders;

2.1.8 be responsible for all environmental considerations within its scope of operations; and 2.1.9 take overall responsibility for environmental issues and for the assessment of corporate environmental objectives, strategies and main processes.

#### **Customer's Environmental Targets**

3.1 The Supplier shall contribute to and assist the Customer in achieving its own sustainability/green targets.

#### Appendix 4 Security Policy

#### **Section 1: Minimum Requirements**

1.1 The security requirements that apply to Government Departments and Service Providers are governed by the Government's core set of mandatory minimum measures to protect information, to apply across central Government of the United Kingdom. Details of the mandatory minimum measures can be found at the Cabinet office website at:

Government Functional Standard GovS 007: Security - GOV.UK (www.gov.uk)

- 1.2 The general requirement is that Service Providers shall be proactive in planning and implementing appropriate policies, processes and procedures to safeguard and protect the information entrusted to them, to enable them to deliver the Service and to demonstrate that they have understood the risks relating to that information and plan mitigating action, which is then put in place and monitored.
- 1.3 As a minimum Service Providers shall put in place specific measures to address the access of Staff and sub-contractors: their organisation's selection and training; systems access rights; the treatment of types of information; and processes for checking compliance.
- 1.4 The CPS is keen to appoint Service Providers that maintain a culture of individual accountability and awareness that encourages staff to be 'trusted stewards' of sensitive data with an obligation to protect it and addresses inappropriate behaviours arising from information mismanagement.
- 1.5 The Service Provider shall hold Cyber Essentials + (plus) and ISO 27001 certification (or the equivalent certifications) to support the delivery of the Services, at contract award. This level of certification must be maintained throughout the duration of the contract.

#### Section 2: Security Classification

- 2.1 The security classification for the CPS's mail will generally be up to Official with the caveat of 'Sensitive' added, as the CPS deals with sensitive material as part of its criminal investigation and prosecution process. The handling of this material may additionally be subject to specific legal requirements.
- 2.2 The Service Provider may be expected to handle mail items consisting of live case data as part of its contracted duties. Under the previous security classifications the possible risks of this type of information were assessed as Impact Level 3 (IL3).
- 2.3 As a Government department, the CPS's' operations are also subject to the Official Secrets Act. The Service Provider shall ensure that all employed Staff engaged to deliver the goods and services sign a declaration pursuant of the Official Secrets Act.

#### **Section 3: Staff Security Requirements**

- 3.1 The CPS deals with criminal prosecutions and the Service Provider must be aware that Service Provider Personnel may be handling live case data. All the Service Provider Personnel connected with the delivery of Service under this Contract shall be vetted to a minimum of BPSS however where heightened access is required, then vetting to SC standard must be considered. Any additional Service Provider Personnel nominated to work on the Contract shall also be vetted in accordance with this standard or higher where appropriate and/or necessary.
- 3.2 The CPS shall carry out periodic spot checks to ensure that the Service Provider Personnel have been security cleared to the appropriate level.
- 3.3 All of the Service Provider Personnel that have the ability to access the CPS's information or systems holding the CPS's information shall undergo regular training on secure information management principles. Unless otherwise agreed with the CPS in writing, this training shall be undertaken annually.
- 3.4 The Service Provider shall ensure that all Sub-Contractors engaged to deliver the goods and services work for a company approved by the CPS and comply with all security requirements.
- 3.5 The Service Provider shall disclose any criminal convictions (both current and spent) to which their Staff have been subject (including motoring conviction) as part of their conditions of employment and will authorise the CPS if required to carry out checks of information provided. The CPS shall have a right to insist that Staff with criminal convictions (excluding minor motoring convictions) are excluded from working on this Contract.

#### **Section 4: General Provisions**

- 4.1 When OFFICIAL level information or higher is held and sorted on the Service Provider premises, the premises in which it is held must be secured. The Service Provider shall ensure that material received at their premises is handled securely, including arrangements for transferring material from the delivery vehicle to the nominated premises.
- 4.2 The Service Provider shall ensure that suitable security measures are used by them to always ensure the security and safekeeping of the CPS's material, including transit.
- 4.3 The Service Provider shall have procedures in place to ensure that any material which is entrusted to their safekeeping is stored securely at all times and not disclosed to unauthorised staff at any time. Applying the 'principle of least privilege' the Service Provider's staff shall only be allowed access to the CPS's mail as required to ensure service delivery.
- 4.4 The Service Provider shall operate an access control system at its premises, via methods such as key codes and dedicated access cards, to ensure that unauthorised individuals cannot access the premises. The Service Provider shall ensure that all windows can be securely locked and operate an alarm system

- 4.5 The Service Provider shall operate a Staff identification process whereby each employee is assigned a unique identifier clearly illustrating designated levels of access.
- 4.6 The Service Provider shall ensure that all material in their possession, in connection with delivery of the Services, is retained in the United Kingdom (UK) and is not stored or processed outside of the United Kingdom.
- 4.7 The Service Provider shall agree any change in location of data storage, processing and administration with the Contracting Body in advance of any proposed move. Contracting Body data shall not be stored outside of the UK unless agreed with the CPS's Senior Security Advisor.
- 4.8 The Service Provider shall allow premises to be inspected by the CPS as required, subject to advance notification, to verify the suitability of security protocols.
- 4.9 Should any of the material relating to the CPS's' business be unaccounted for whilst in the care of the Service Provider, the Service Provider shall trace this material within forty-eight (48) hours. Loss of any material shall be treated as a serious breach of security. Any such loss should be reported within twenty-four (24) hours to the CPS's Operational Security Team.
- 4.10 The Service Provider shall appreciate that public sector document provenance and data sharing security may, on occasion, be of interest to various sectors of the media. Under no circumstances should any of the CPS's' information be disclosed to external sources.
- 4.11 The Service Provider shall provide staff and documentation at the discretion of the CPS to demonstrate that document provenance and data sharing is robustly managed and is secure.
- 4.12 The Service Provider shall ensure that normal security standards are maintained in the event of a business continuity issue.
- 4.13 If the Service Provider receives a Right of Access (ROAR) application under the Data Protection Act (DPA) and/or the Freedom of Information (FOI) Act any such application must be notified to the CPS Representative and referred to the CPS Information Access Team's inbox before any response is made. All other DPA rights requests should be referred to the Data Protection Officer's inbox

# Section 5: Information Security Protocols

5.1 If any CPS information is held and accessed within Service Provider systems, the Service Provider shall comply with at least the minimum set of security measures and standards as determined by the Government Functional Standard GovS007 <u>https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach</u>

ment data/file/1016424/GovS 007- Security.pdf as well as any additional protections as needed as a result of their risk assessment.

5.2 Should any service provider utilise Cloud Services in the IT deliverables then they must conform the requirements in line with NCSC's 14 Cloud Principles.

#### The cloud security principles - NCSC.GOV.UK

5.3 Unless otherwise agreed with the CPS in writing, all Service Provider devices used to access or manage CPS information are expected to meet the set of security requirements set out in the NCSC End User Devices Security Guidance or its successor:

#### Device Security Guidance - NCSC.GOV.UK

- 5.4 Wherever possible, such information shall be held and accessed on ICT systems on secure premises. This means Service Provider shall avoid use of removable media (including laptops, portable hard drives, CDs, USB memory sticks, tablets and media card formats) for storage or access to such data where possible.
- 5.5 Where it is not possible to avoid the use of removable media, Service Provider shall apply all of the following conditions:
  - The information transferred to the removable media shall be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the information and the scope of information held. Where possible, only anonymised information shall be held;
  - user rights to transfer data to removable media shall be carefully considered and strictly limited to ensure that this is only provided where absolutely necessary for business purposes and subject to monitoring by managers, and
  - The individual responsible for the removable media shall handle it themselves or if they entrust it to others as if it were the equivalent of a large amount of their own cash.
  - The data shall be encrypted to a UK Government standard appropriate for handling data up to and including OFFICIAL-SENSITIVE, or FIPS 140-2, using software that does not require a software download onto the recipient's device.
  - The data contained on the media shall be securely erased as soon as it has been transferred to a secure source.
- 5.6 When CPS data is held on mobile, removable or physically uncontrolled devices or portable media, such as laptops or tablets, it shall be stored and encrypted to a UK

Government standard appropriate for handling data up to and including OFFICIAL-SENSITIVE, such as FIPS 140-2 or NCSC approved methods.

- 5.7 Where the Service Provider grants increased IT privileges or access rights to its Staff or Sub-contractors, those persons shall be granted only those permissions necessary for them to carry out their duties and be subject to appropriate monitoring. When Staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.
- 5.8 Service Provider shall recognise the need for the Contracting Body's information to be safeguarded under the UK Data Protection regime. To that end, Service Provider shall be able to state to the CPS the physical locations in which data may be stored, processed and managed from, and to confirm that all relevant legal and regulatory frameworks authority are complied with.
- 5.9 Service Provider shall agree any change in location of data storage, processing and administration with the CPS in advance of any proposed move to the extent that such move has any impact upon the Service and relates specifically to the CPS Data. CPS Data shall not be stored outside of the UK unless agreed with the CPS's Senior Security Advisor.
- 5.10 The CPS requires that any information up to Official Sensitive transmitted electronically shall be sent via the Criminal Justice Secure Email (CJSM) system. The CPS will sponsor and pay for Service Provider's subscription to this system. The CJSM service is an important part of the process of joining up the Criminal Justice System (CJS) in England and Wales. It allows people working in the CJS to send emails containing information up to OFFICIAL SENSITIVE in a secure way. CJSM uses a dedicated server to securely transmit emails between connected criminal justice practitioners. Once connected, users can use CJSM to send secure emails to each other and to criminal justice organisations. As the ICT infrastructure of the CPS is updated during the course of the Contract, Service Provider may be required to transmit data via other electronic systems, such as the 'Egress' system, but this should be agreed with the CPS Senior Security Advisor.

**Revised April 2023** 

#### Appendix 5 – Schedules

#### **Call-Off Schedules**

Call-Off Schedule 1 (Transparency Reports)



RM1043.8\_Call-Off-S chedule-1-Transpare

#### Call-Off Schedule 3 (Continuous Improvement)



RM1043.8\_Call-Off-S chedule-3-Continuo

Call-Off Schedule 5 (Pricing Details and Expenses Policy)



RM1043.8\_Call-Off-S chedule-5-Pricing-D

# Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)



#### Call-Off Schedule 7 (Key Supplier Staff)



#### Call-Off Schedule 9 (Security)



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



Call-Off Schedule 18 (Background Checks)



Call-Off Schedule 20 (Call-Off Specification)



# Call-Off Schedule 25 (Ethical Walls Agreement)



RM1043.8\_Call-Off-S chedule-25-Ethical-V

#### Call-Off Schedule 26 (Cyber Essentials Scheme)



#### **Joint Schedules**

Joint Schedule 2 (Variation Form)



Joint Schedule 3 (Insurance Requirements)



Joint Schedule 4 (Commercially Sensitive Information)



#### Joint Schedule 10 (Rectification Plan)



RM1043.8\_Joint-Sch edule-10-Rectificatio

Joint Schedule 11 (Processing Data) RM1043.8



RM1043.8\_Joint-Sch edule-11 Processing