

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2018

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

Order Form

CALL-OFF REFERENCE: **PRO 5593**THE BUYER: Secretary of State for Health and Social Care
acting as part of the Crown through the UK Health
Security Agency

BUYER ADDRESS Nobel House, Smith Square, London, SW1P 3HX

THE SUPPLIER: Anexsys Limited

SUPPLIER ADDRESS: 3rd Floor, 10 Aldersgate Street, London,
England, EC1A 4HJ

REGISTRATION NUMBER: [REDACTED]

DUNS NUMBER: [REDACTED]

SID4GOV ID: **N/A**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 19 April 2023.

It's issued under the Framework Contract with the reference number RM6203 for the provision of eDisclosure and Review Services.

CALL-OFF LOT(S):

Lot 4: [REDACTED]

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 and Interpretation) RM6203
3. The following Schedules in equal order of precedence:
 - Joint Schedules for **RM6203**
 - o Joint Schedule 2 (Variation Form)

Framework Ref: RM6203

Project Version: v1.0

Model Version: v3.8

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

- o Joint Schedule 3 (Insurance Requirements)
- o Joint Schedule 4 (Commercially Sensitive Information)
- o Joint Schedule 10 (Rectification Plan)
- o Joint Schedule 11 (Processing Data)
- o
- Call-Off Schedules for PRO 5593
 - o Call-off Schedule 1 (Transparency Reports)
 - o Call-off Schedule 3 (Continuous Improvement)
 - o Call-off Schedule 5 (Pricing Details)
 - o Call-off Schedule 6 (ICT Services)
 - o Call-off Schedule 7 (Key Supplier Staff)
 - o Call-off Schedule 8 (Business Continuity and Disaster Recovery)
 - o Call-off Schedule 9 (Security)
 - o Call-off Schedule 10 (Exit Management)
 - o Call-off Schedule 13 (Implementation plan and testing)
 - o Call-off Schedule 14 (Service Levels)
 - o Call-off Schedule 15 (Call-Off Contract Management)
 - o Call-off Schedule 16 (Benchmarking)
 - o Call-off Schedule 18 (Background Checks)
 - o Call-off Schedule 20 (Call-Off Specification)
- 4. CCS Core Terms (version 3.0.8)
- 5. Joint Schedule 5 (Corporate Social Responsibility) RM6203
- 6. 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.
- 7. Appendix A – Cyber Security Mandatory Requirements
- 8. Appendix B – Statement of Work (SOW) template

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

CALL-OFF SPECIAL TERMS

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

None

CALL-OFF START DATE: 20 April 2023

CALL-OFF EXPIRY DATE: 19 April 2025

CALL-OFF INITIAL PERIOD: 2 years

OPTIONAL EXTENSION PERIOD: 1 year

BREAK CLAUSE

N/A

CALL-OFF DELIVERABLES

Framework Ref: RM6203

Project Version: v1.0

Model Version: v3.8

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

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

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is [REDACTED] in the first 12 months of the Contract.

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)

The total charges under this Call-Off Order shall not exceed £1,257,100 ex VAT (one-million two-hundred-and-fifty seven thousand and one-hundred pounds sterling).

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Monthly in arrears by BACS or alternative payment method as agreed between the Buyer and the Supplier. Submitted invoices must be accompanied by supporting information including:

- completed timesheets for amounts set out in the relevant invoice; and
- such other information as the Buyer (acting reasonably) may require in order to verify the invoiced amounts.

BUYER'S INVOICE ADDRESS:

[REDACTED]

Accounts Payable;
UK Health Security Agency,
Manor Farm Road,
Porton Down,
Salisbury,
SP4 0JG UKHSA

VAT No: [REDACTED]

Contact number for all invoice related queries: [REDACTED] Please select Option 5, and then Option 1

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

BUYER'S ENVIRONMENTAL POLICY

Framework Ref: RM6203
Project Version: v1.0
Model Version: v3.8

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

N/A

BUYER'S SECURITY POLICY

N/A

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

SUPPLIER'S CONTRACT MANAGER

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY

Quarterly on the first Working Day of each quarter

KEY STAFF

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

KEY SUBCONTRACTOR(S)

[REDACTED]

COMMERCIALLY SENSITIVE INFORMATION

Supplier's Commercially Sensitive Information

SERVICE CREDITS

Service Credits will accrue in accordance with Call-Off Schedule 14 (Service Levels).

In relation to the processing of data, a Critical Service Level Failure shall comprise a failure to process electronic material within [REDACTED] from receipt or hard copy within [REDACTED] of receipt.

In relation to availability of the eDisclosure review platform, a Critical Service Level Failure shall comprise the system not being available [REDACTED] of the time during [REDACTED] and [REDACTED] at all other times [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

ADDITIONAL INSURANCES

The Supplier shall produce architecture and design artefacts to the level of depth and quality to gain approval through UKHSA and CDDO technical review assurance, with suppliers responsible for presenting architecture and designs for approval and refining those as needed to gain governance approvals. Supplier must comply with the UKHSA governance process.

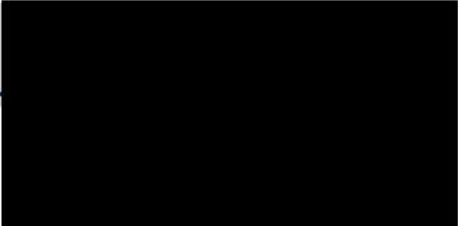
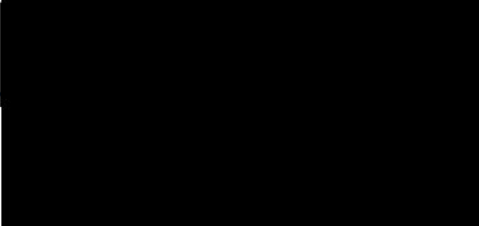
The Supplier shall provide evidence that the final product website can meet WCAG 2.1 AA accessibility standard, that the supplier can conduct a WCAG 2.1 review to verify that (either by themselves internally or independently) and should be able to allow for third party / UKHSA deeper reviews if needed, and that the supplier can publish an accessibility statement within the final product website.

GUARANTEE

There's a guarantee of the Supplier's performance provided for all Call-Off Contracts entered under the Framework Contract.

SOCIAL VALUE COMMITMENT

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

For and on behalf of the Supplier:	For and on behalf of the Buyer:
<p>DocuSigned by:</p>  <p>Date Signed: 20/04/2023</p>	<p>DocuSigned by:</p>  <p>Date Signed: 24/04/2023</p>

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2018

Appendix A – Cyber Security Mandatory Requirements

1	Governance	
1.1	Cyber Essentials.	The Supplier shall hold, before the commencement of this contract, and maintain throughout the duration of the contract, certification to the NCSC Cyber Essentials or NCSC Cyber Essentials Plus where information classified as Official Sensitive is stored, accessed or processed.
1.2a	The contract shall mandate the management of cyber security via an ISO27001-aligned governance structure.	An Information Security Management System, including an improvement plan, shall be developed and maintained, structured in accordance with ISO27001:2013 or at least Version 3.1 of the NCSC Cyber Assessment Framework, to cover all Information Assurance aspects of the Supplier and their Systems throughout the life of the contract. This will include, but is not limited to: scope; statement of applicability; risk management plans and other artefacts all of which shall be agreed with the Authority.
1.2b	The contract shall mandate the management of cyber security via an ISO27001-aligned governance structure.	The Information Security Management System shall be presented to the Authority for approval within twenty (20) working days of contract signature.
1.3	The supplier shall accept that their governance will align to UKHSA cyber security policies and standards.	The Supplier Information Security Management System and associated policies shall be compliant with the Authority's core cyber security policies and standards unless a pre-agreed exemption has been obtained from the Head of Cyber Security.
1.4	The scope of the cyber governance shall include all core service management areas.	The Supplier Information Security Management System shall have within its scope all service management activities and related systems managed by the Supplier, including but not limited to change management, incident management, and other service management artefacts aligned with ISO20000 or ITIL.
1.5a	The Information Security Management System shall be reviewed annually and improvements agreed with the Authority.	The Supplier Information Security Management System shall be fully reviewed and updated by the Supplier at least annually to reflect: (a) industry changes in accepted good practices including revisions to ISO27001 and NCSC CAF; (b) changes to the System; (c) changes to the Authority's security policies; (d) changes to the Authority's threat landscape including security

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

		incidents at the Supplier or any sub-contractors; (e) any other reasonable changes requested by the Authority.
1.5b	The Supplier shall provide the output from the annual Information Security Management System review to the Authority.	The Supplier shall provide the Authority with the output of these reviews as soon as is practically possible and no later than twenty (20) working days after the review, detailing suggested improvements for agreement with the Authority.
1.6	Formal ownership of cyber security, within the supplier, and specifically for this service or delivery, shall be specified in the contract.	There shall be a named person from the Supplier who is accountable for the provision of technical, personnel, process and physical security aspects for the scope of the contract, including but not limited to security clearances. This named accountable person shall be formally communicated to the Authority within ten (10) days of contract signature. The nominated person shall of sufficient seniority within the Supplier to have direct access to Supplier executive management.
1.7	The Supplier shall engage with the Authority's Cyber Security Assurance Processes	The Supplier agrees to engage and co-operate with the Authority's Cyber Security assurance processes as required. These will include but not be limited to: <ul style="list-style-type: none"> • Supplier Assurance • Product Assurance • Training Assurance, including materials and completions.
1.8a	The right of audit shall be provided.	The Authority or its agents, or HMG appointed internal or external audit teams may undertake reviews and technical testing of the security controls in place around the Supplier's Systems and Services. This will include the right to audit and assess security controls at any of the sites and on any of the systems used for the purpose of meeting the contract. Where such sites or systems are provided by sub-contractors, the Supplier will ensure that this requirement is flowed down in to contracts between the Supplier and such subcontractors.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

1.8b	The right of audit shall be provided.	Where physical or access is unavailable due to provision by use of cloud service, or by other agreed exceptional circumstances or contractual issues, suitably trustworthy independent assessments of the security in question shall be made available. As part of this audit requirement, the Supplier shall consistently engage with the Authority's preferred process for undertaking supplier due diligence activities.
1.8c	The right to audit shall be provided.	Reviews undertaken by the Authority on any one element of the Supplier's solution will usually be limited to pre-release and annual post-release reviews, unless the site or service has been materially involved in a cyber or other security incident. In such cases, out of cycle reviews can be undertaken in addition to any annual review.
1.8d	The right to audit shall be provided.	The Authority reserves the right to Audit Supply Chain security measures applied in context of the risks to the Sites, Facilities and services within the scope of the Agreement, including those security measures under the governance of the Supplier, or any of its Sub-contractors.
1.9	The contract shall mandate compliance with relevant laws.	The Supplier shall ensure that the systems or services are delivered (include design, implementation and operation as relevant) in compliance with the requirements of UK and, if applicable, local law. Any discrepancies are to be notified to the Authority within one working day of the Supplier becoming aware of such.
1.10	Cyber security good standard practices as well as HMG standards and guidelines should be referenced for development and testing where relevant.	The System shall be developed in line with and reviewed against agreed good practices for cyber security. Assurance of this shall be undertaken by the Supplier via regular review activities including security and vulnerability testing of the infrastructure and applications, and code reviews and CI/CD pipeline assurance (where relevant).
1.11	A risk assessment shall be undertaken and maintained by the supplier, and its methodology shared with UKHSA.	The Supplier shall undertake a risk assessment of the whole System and supporting processes in line with the Information Security Management System and the Authority's Standards, and refresh those assessments when system changes are made. The Authority retains the rights to review and approve the repeatable methodology used for risk assessment.
1.12	The supplier shall agree to share the outputs from	The Supplier shall share with the Authority the outputs of the risk assessment for the product or services, including mitigation actions and any remaining remediation plans.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

	initial and ongoing risk assessments, including mitigation plans and the like.	
1.13	Structures shall be in place to ensure interworking between the Supplier and UKHSA to ensure alignment over risk management, etc.	The Supplier shall engage with the Authority with regards to managing all security-related risks to ensure they are within the Authority's risk appetite and tolerances or there is a risk exception acceptance in writing from the Authority. As a minimum this will be through active attendance at the nominated Security Working Group.
1.14	Geographical access to production data.	The Supplier will ensure that all production data is resident and processed within the UK and access to such data is only granted to staff based in the UK. This is to include access to backup and archive copies of production data. (Note, this is separate to GDPR requirements for geographical limitations on processing personal data.)
2	Awareness & Training	
2.1	Suppliers shall be maintaining a suitable awareness and training program.	All Supplier staff & subcontractor users and relevant employees shall be provided with appropriate security education, training and awareness by the Supplier, with this aspect being reviewed at least annually and whenever personnel roles change. Training shall include elements of physical, personnel and electronic security guidance.
2.2	Suppliers shall sign on to take UKHSA training where requested.	All staff, subcontractor's users and relevant employees shall undertake any further training provided by the Authority for the Authority's staff or suppliers, as requested by the Authority.
3	Personnel Security	
3.1	SC-level clearance shall be agreed for all supplier staff and subcontractors with access to UKHSA systems or data.	The Supplier will provide screening controls that conform to the Security Cleared (SC) Security Standard for all staff and subcontractors who have any physical or logical access to production systems or data. There may be a requirement for enhanced UK Security Vetting clearances for certain roles, based on the Authority's risk assessment and management.
4	Operational Security	
4.1	Operational security monitoring shall be in place.	Where the Supplier does not fully integrate with the Authority's security event and incident monitoring and management processes, the Supplier will have implemented and practiced security operational awareness, detection, prevention, response and remediation processes and

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

		controls to effectively manage security incidents before commencing work for the Authority.
4.2	UKHSA security compliance findings will be remediated.	Where the Supplier's systems or services are hosted on the Authority's environments, security defects, vulnerabilities and other non-compliances identified by the Authority's compliance technologies will be remediated within 15 days unless the Authority exceptionally accepts in writing that findings that will not be addressed.
4.3	Ongoing assurance activities shall be undertaken by the supplier (penetration testing, scans, etc) and the output of those activities actively managed.	The Supplier will conduct at least annually or more frequently if required (e.g. PCI-DSS compliance), vulnerability, security, and penetration testing and, address the findings of these activities or have the Authority accept in writing that findings that will not be addressed.
4.4	Additional assurance activities shall be undertaken when requested (typically at cost).	The Supplier shall facilitate requests by the Authority to undertake testing and assurance activities by the Authority, service providers acting on the Authority's behalf or HMG audit bodies.
5	Security Architectural Principles	
5.1	Architectural controls to protect the live environment shall be in place	Development and test environments shall have assured separation from the live/production systems, and shall not use live / production information without prior written Authority approval.
5.2	Least privilege based access controls are required at both an ICT and physical level	The System and locations shall have auditable authorisation, authentication and access control based on least privilege, and aligned appropriate to the business requirement.
5.3	Role-based separation of duties shall be in place wherever possible	The System and processes shall enforce separation of duties based upon the agreed risk assessment and management controls. The Supplier shall ensure that the System and associated infrastructure is designed in a manner to ensure effective physical and logical separation, including but not limited to: <ul style="list-style-type: none"> • Production and back office networks and services shall be appropriately segregated. • Privileged users shall be provided with separate accounts or roles for normal and privileged activities.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

		<ul style="list-style-type: none"> • All internet and privileged access shall be protected by strong authentication (including as MFA) and additional necessary controls.
5.4	Appropriate encryption shall be applied to all data in transit and at rest.	Except where explicitly permitted by the Authority in an approved Low Level Design, all Authority production data will be subject to appropriate encryption. This includes data in transit and at rest, and on removable media of any sort. Backups and archives of production data are to be similarly protected. Advice on appropriate algorithm and key length options for any specific scenario can be sought from the Authority's Cyber Security Team.
5.5	Access only via approved technologies.	Access to the Authority's data, services and platforms will only be permitted using the Authority's approved methods, such as the Authority's managed virtual devices, or exceptionally, using the Authority's supplied physical Information Technology assets. Access using non-approved methods may be terminated and blocked without notice.
6	Protective Monitoring	
6.1	UKHSA monitoring shall be used for systems or services hosted on UKHSA environments.	Where the Supplier's systems or services are hosted on the Authority's environments, security and operational monitoring will be provided using the Authority's approved technologies and the Supplier will ensure that these are effectively integrated.
6.2a	Protective monitoring shall be in place via integration with UKHSA monitoring	The Supplier shall integrate externally hosted systems or services with the Authority's preferred Protective Monitoring capability, Microsoft Sentinel, or provide their own which is recognised as at least as capable as the former.
6.2b	Protective monitoring shall be in place without integration with UKHSA monitoring	The Supplier shall integrate externally hosted systems or services with their own which is recognised as at least as capable as the Authority's preferred Protective Monitoring capability. The Supplier shall be capable of integrating with the Authority's wider incident response

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

		<p>capability to ensure an appropriate level of visibility is being maintained.</p> <p>The Supplier shall ingest logs continuously/dynamically into the Authority's preferred Protective Monitoring capability, Microsoft Sentinel.</p>
7	Incident Response	
7.1	Incident response management shall be in place, and SLAs shall be defined around both overall management and the UKHSA Cyber Security team.	The Supplier shall integrate with the Authority's incident management processes. Where the Supplier becomes aware of a potential cyber security incident which may impact systems, services, or data being provided to or maintained on behalf of the Authority, these shall be raised to the Authority in line with the Authority's Cyber Security Incident Reporting Policy. Processes around this interaction shall be detailed within the Supplier Information Security Management System.
7.2	Contact details for 24x7 and holiday incident management shall be contractually specified.	An Incident Management hotline number and set of contacts shall be provided to the Authority by the Supplier, and availability of contacts shall be maintained in line with the service level agreements between the Supplier and the Authority. These contact details and associated number(s) will be provided to the Authority prior to the commencement of production Systems or Services being in place.
8	Contract Closure	
8.1	On completion of contract all sensitive UKHSA data will be securely removed from supplier systems.	<p>All data stores are to be identified during the operation of the services or systems and upon completion of the contract, the supplier is to securely delete (or, otherwise, destroy) all Authority data (which will include all personal data and special category personal data where there is not an explicit legal justification for retention). This will include online and off-line backup and any archive not maintained by the Authority.</p> <p>Upon contract closure, the Supplier shall provide an appropriate Certificate of data destruction to the Authority with reference to the relevant industry standards.</p>

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

Appendix B – Statement of Work Template**Statement of Work****1. Statement of Works (SOW) Details**

Upon execution, this SOW forms part of the Call-Off Contract PRO 5593 Framework Schedule 6 Order Form - Anexsys Ltd.

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

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

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

Date of SOW:	
SOW Title:	
SOW Reference:	
Call-Off Contract Reference:	
Buyer:	The UK Health Security Agency (UKHSA)
Supplier:	Anexsys Limited
SOW Start Date:	
SOW End Date:	
Duration of SOW:	As per dates stated above.
Key Personnel (Buyer):	
Key Personnel (Supplier):	
Subcontractors:	N/A

2. Call-Off Contract Specification – Deliverables Context SOW Deliverables Background

Key Deliverables of this SOW:	<ul style="list-style-type: none"> • • • • •
Delivery phase(s):	Procurement
Overview of Requirement:	Delivery - To plan, manage and deliver the end-to-end delivery of a defined set of business outcomes

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

3. Buyer Requirements – SOW Deliverables Outcome Description:

Milestone Ref	Milestone Description	Acceptance Criteria	Due Date
MS01			
MS02			
MS03			

Delivery Plan:**Dependencies:**

Notable supplier deliverables which constitute dependencies to this SoW includes the supplier's mobilisation plan.

Supplier Resource Plan:**Security Applicable to SOW:**

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with section 3.1 of Appendix A – Cyber Security Mandatory Requirements of this Call-Off Order.

Cyber Essentials Scheme:

The Buyer requires the Supplier to have and maintain a **Cyber Essentials Certificate** for the work undertaken under this SOW, in accordance with RM6203 Framework Schedule 9 (Cyber Essentials Scheme).

SOW Standards:

N/A

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

Performance Management:

Material KPIs	Target	Measured by
1. Performance Reports – summary for each Milestone, including: <ul style="list-style-type: none"> a. overall mgt headlines b. key achievements in this period c. key activities for next period d. Risks, Issues, escalations e. Deliverables / Milestones f. Rag Status 2. Summary of Contract including variations: <ul style="list-style-type: none"> a. Workstream Ref No b. Contract Value c. Start / end date 3. Contract financial forecast: <ul style="list-style-type: none"> a. SOW name b. Value c. Invoiced to date d. Forecast to end date e. Total spend forecast 4. Contract Invoice Status	Timeframe	.
5. Resource Profile <ul style="list-style-type: none"> a. Workstream b. Name c. Role d. Ratecard e. Start date 		
End date		
Call-Off Contract Charges	The supplier provides these monthly	Submitted timely and contain accurate and complete information
Balanced Score Card Template and measurements - to be agreed within 4 weeks of Contract Start Date	To be agreed within 4 weeks of SOW Start Date	To be agreed within 4 weeks of SOW Start Date

Additional Requirements:

Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract applies.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

Key Supplier Staff:

Key Role	Key Staff	Contract Details	Employment / Engagement Route (incl. inside/outside IR35)

SOW Reporting Requirements:

Further to the Supplier providing the management information detailed in Paragraph 6 of Call-Off Schedule 15 (Call Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:

Ref	Type of Information	Which Services does this requirement apply to?	Required regularity of Submission
1.	Delivery Phase		
1.1	1. Performance report – summary for each stream including <ul style="list-style-type: none"> a. overall mgt headlines b. key achievements in this period c. key activities for next period d. Risks, Issues, escalation s e. Deliverables / Milestone s f. Rag Status 2. Summary of Contract including variations <ul style="list-style-type: none"> a. Workstream Ref No b. Contract Value c. Start / 3. Contract financial forecast <ul style="list-style-type: none"> a. SOW name b. Value c. Invoiced to date d. Forecast to end date e. Total spend forecast 4. Contract invoice Status	Delivery Phase	Weekly

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

	5. Resource profile a. Workstream b. Name c. Role d. Rate card e. Start date 6. End date	
--	--	--

4. Charges**Call Off Contract Charges:**

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

- 1 Capped Statement of Work (SOW)

The Hourly Rate charged shall not exceed 7.5 hours per day, unless where agreed in writing by the Buyer.

#	Staff Name	Role	SFIA	Rate	Days	Fee
1	TBC		Grade	■	■	■
2						
3						
4						
5						
6						
						£

Rate Cards Applicable: See Call-Off Schedule 5 (Pricing Details)

5. Signatures and Approvals Agreement of this SOW

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

An Authorised Signatory for the Supplier:	An Authorised Signatory for the Buyer: