DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	[redacted]
THE BUYER:	The Secretary of State for the Home Department (acting through the Home Office)
BUYER ADDRESS	The Secretary of State for the Home Department, 2 Marsham Street, 4th Floor Peel London, SW1P 4DF
THE SUPPLIER:	KPMG LLP
SUPPLIER ADDRESS:	15 Canada Square, London, E14 5GL
REGISTRATION NUMBER:	OC301540
DUNS NUMBER:	[redacted]

DPS SUPPLIER REGISTRATION SERVICE ID: [if known]

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 15th December 2024
It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
Non-assured NCSC Services, Risk Management, Risk Assessment, Audit and Review, Business Continuity and Disaster Recovery - BCDR, Security Specialist, Security Supply Chain Analysis, Security Strategy, Cyber Transformation, Policy Development, Cyber Essentials Plus, Clearance: Security Check, ISO 27001

ORDER INCORPORATED TERMS
The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM3764iii
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 7 (Financial Difficulties)
        - Joint Schedule 10 (Rectification Plan)

    - Order Schedules for RM3764iii
        - Order Schedule 2 (Staff Transfer) – Part C
        - Order Schedule 4 (Order Tender)
        - Order Schedule 5 (Pricing Details)
        - Order Schedule 7 (Key Supplier Staff)
        - Order Schedule 8 (Business Continuity and Disaster Recovery)
        - Order Schedule 9 (Security) - Part A
        - Order Schedule 10 (Exit Management)
        - Order Schedule 15 (Order Contract Management)
        - Order Schedule 18 (Background Checks)
        - Order Schedule 20 (Order Specification)
4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6
7. Order Schedule 4 (Order Tender) as long as any parts of the Order Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

ORDER SPECIAL TERMS N/A
The following Special Terms are incorporated into this Order Contract:
None

ORDER START DATE:	Expected 16th December 2024
ORDER EXPIRY DATE:	Expected 15th December 2026
ORDER INITIAL PERIOD:	2 Years
ORDER OPTIONAL EXTENSION	2 period of 12 months

DELIVERABLES:
As stated in individual Statement of Works (SoW)

MAXIMUM LIABILITY

[redacted]

ORDER CHARGES

See details in Order Schedule 5 (Pricing Details) – See Annex C.

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract: N/A

PAYMENT METHOD
Payment for this Call-Off is monthly by BACS

BUYER'S INVOICE ADDRESS:
Invoices will be sent via email as the primary method for delivery to the address below:

HOCyberSecurity-BizOps@homeoffice.gov.uk

hosupplierinvoices@homeoffice.gov.uk

Invoices can be submitted in hard copy via post to the address below, however this will significantly delay the processing of the payment to the Supplier.
Home Office Shared Service Centre

[redacted]

The Buyer shall accept and process for payment an electronic invoice submitted for payment by the Supplier where the invoice is undisputed and where it complies with the standard on electronic invoicing.

For the purposes of paragraph above, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.

All invoices must include:

- A valid Purchase Order number
- The contract reference number [redacted]
- The period of time pertaining to the Charges included on the invoice.
- A summary of the corresponding Services.
- The value of the VAT portion of the invoice expressed in Pounds Sterling.
- Invoices should be submitted via email in pdf, tiff, jpeg or png format (Excel is not supported):
- a multipage invoice should be sent by the Supplier as one attachment to the email, however multiple invoices should be split across different attachments (1 attachment equals 1 invoice)
- multiple invoices can be attached to one email up to a maximum size of 5mb
- the supplier should be aware that any text in the body of their email, or attachments submitted in files formats other than those listed above will not be read by anyone.

BUYER'S AUTHORISED REPRESENTATIVE:

[redacted]

BUYER'S ENVIRONMENTAL POLICY

https://www.gov.uk/government/publications/greeninggovernment-commitments-2016-to-2020/greening-government-commitments-2016-to-2020

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

BUYER'S SECURITY POLICY

Home Office
Security Policy for Cc

https://www.gov.uk/government/publications/security-policy-framework
https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

SUPPLIER'S AUTHORISED REPRESENTATIVE

[redacted]

SUPPLIER'S CONTRACT MANAGER

[redacted]

PROGRESS REPORT FREQUENCY
Monthly

PROGRESS MEETING FREQUENCY
Weekly

KEY STAFF

[redacted]

KEY SUBCONTRACTOR(S)
N/A

COMMERCIALLY SENSITIVE INFORMATION: TBC
Supplier's Commercially Sensitive Information

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not Applicable

SOCIAL VALUE COMMITMENT
The supplier will deliver social value commitment laid out in the Social Value Section of [redacted] commitment provided in below

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

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:	[redacted]	Name:	[redacted]
Role:	[redacted]	Role:	[redacted]
Date:	11.12.2024	Date:	12/12/24

1. SCOPE OF REQUIREMENT

1.1. Detailed below is an outline of the requirement stating what is in scope:

1.1.1. The work packages that are in scope of this requirement are;

1.1.1.1. WP1: Embed Cyber Risk Management and Governance across Home Office.
1.1.1.2. WP2: Establish People, Culture and Training baseline.
1.1.1.3. WP3: Develop Cyber Risk Capacity
1.1.1.4. WP4: Arms-Lengths Bodies & Wider Ecosystem Governance Model.
1.1.1.5. WP5: Risk Management and Controls Automation.
1.1.1.6. WP6: Enhance the Framework.
1.1.1.7. WP7: Maturing the Risk Management Framework.
1.1.1.8. WP8: Develop Cyber risk data model and reporting capabilities.

2. THE REQUIREMENT

2.1. WP1: Embed Cyber Risk Management and Governance.

2.1.1. Drive adoption of Cyber Risk management across Home Office, maturing a consistent governance structure across projects, programmes, business areas and portfolios. This workstream is intended to bring Home Office business areas and portfolios into alignment for managing cyber risk in accordance with HOCS policy, enabling the Home Office to maintain and develop a coherent view of its risk posture. It includes assessment of the key strategic cyber risks as driven by critical services to achieve a baseline quantification of the risks.

2.1.2. The delivery partner is expected to work with business areas and portfolios across Home Office to help them understand the cyber risk for their essential services and then support them in quantifying and reporting the risk.

2.1.3. Key Outputs.

2.1.3.1. Cross-Home Office adoption of Cyber Risk Management and reporting in accordance with the governance structure.
2.1.3.2. Embedding plan and roadmap including metrics for measuring adoption.
2.1.3.3. Adoption report documenting adoption progress and including lessons learned.
2.1.3.4. Metrics and associated strategy to measure the effectiveness of the Framework in reducing cyber risk.
2.1.3.5. Maturity quantification of cyber risk aligned to critical services/systems
2.1.3.6. Provide context to the results of cyber risk quantification through comparison with wider industry.
2.1.3.7. Establish the ability the assess Cyber Risk Controls using

ServiceNow.

2.1.3.8. Define Cyber Risk targets with Portfolio risk owners. Ensuring ownership, accountability and empowerment to deliver them.

2.2. WP2: Establish People, Culture and Training baseline.

2.2.1. This workstream is intended to identify existing cyber risk communities and establish a proactive and engaged cyber risk culture across Home Office, unique to Home Office. Carry out an assessment to develop the cyber risk culture baseline and use the assessment to define targeted initiatives aligned to wider Home Office outputs. Embed board-level exercising into BAU (Business as Usual) for measuring effectiveness of risk reduction initiatives while establishing the training plans and skills development areas.

2.2.2. With a large number of business areas and portfolios, active projects and varying levels of cyber risk management maturity, the delivery partner is expected to provide a clear and coherent strategy for enhancing cyber risk culture, quickly and effectively across the Home Office. Siloed working practices and key non-cyber business objectives have resulted in fragmentation. A willingness to improve is part of Home Office culture and the delivery partner is expected to leverage this in support of delivering the required outputs.

2.2.3. Key Outputs.

2.2.3.1. Cyber Risk Culture assessment report.
2.2.3.2. Document initiatives to enhance the culture.
2.2.3.3. Training plan for identified skills development areas.
2.2.3.4. Reporting template for culture management information.
2.2.3.5. Report documenting the recommendations for aligning the training pathways to the framework
2.2.3.6. Board exercising strategy signed off by board representatives.
2.2.3.7. Strategy for identifying and resolving non-standard cyber issues.

2.3. WP3: Develop Cyber Risk Capacity

2.3.1. This workstream is intended to develop, quantify and deliver a centralised risk management capability in accordance with the cyber risk management framework

2.3.2. The delivery partner is expected to manage and maintain an operating model for the HOCS GRC capability, focused on Risk Management and detailing functional processes aligned to leading practices, tools and technology compatible with the processes, people, their skills and their interaction with the processes, a governance approach including associated policies and a capability for reporting KPIs and benchmarking.

2.3.3. Key Outputs:

2.3.3.1. Review effectiveness of Operating model and define set of recommendations and changes to improve.

2.3.3.2. Proposed enhancements to HO GRC Op Model to enable effective roll-out to ALBs (see WP4)

2.4. WP4: Arms-Length Bodies/Wider Ecosystem Governance Model.

2.4.1. This workstream is intended to outline the approach to influencing cross-government adoption of good cyber risk management. As the nominated lead government department for Cyber Security, the Home Office has a key role for driving compliance to the UK government cyber security strategy. Based on the learnings from embedding cyber risk management across Home Office, the delivery partner is expected to develop a Cyber Risk Governance model for the Arms-Length Bodies across Government. Share the governance model and risk management approach across government departments and define a strategy for embedding.

2.4.2. Key Outputs:

2.4.2.1. A framework for ALB and ecosystem cyber risk management.

2.4.2.2. A strategy and roadmap for embedding the proposed ALB Cyber risk management framework

2.5. WP5: Risk Management and Controls Automation (ServiceNow)

2.5.1. This workstream is intended to enhance the level of capability that the current ServiceNow instance provides for Cyber Risk Management.

2.5.2. The delivery partner will need to develop the roadmap for automation capability growth and adoption, identifying the required automation architecture and technical design based on defined user personas and a functional design and considering third party cyber risk management.

2.5.3. The delivery partner will need to design automated reporting and a user interfaces for each of the personas.

2.5.4. The delivery partner will be required to develop the design and conduct quality assurance and acceptance testing for the delivered capability as well as artefacts for business change management.

2.5.5. The delivery partner will be required to work with incumbents in cyber governance and cyber compliance teams to capture requirements and ensure compatibility with GRC processes in the tool.

2.5.6. Key Outputs.

2.5.6.1. A plan for business adoption of new capability.
2.5.6.2. Phased delivery approach to the ServiceNow capability defined in the risk framework, delivered in multiple releases throughout the project.
2.5.6.3. Developer resource required to construct the technical architecture of ServiceNow ready for deployment.

2.6. WP6: Enhance the Framework

2.6.1. This workstream is intended to provide additional capabilities for cyber risk management through establishing a number of capabilities to inform risk management decisions, and capabilities to inform risk process.
2.6.2. Enhance the existing controls library to include controls baseline, metrics for defining effectiveness and ensure integrated with the tooling approach taken under WP5.
2.6.3. Establish a third-party risk management capability feed into the cyber risk management process.

2.6.4. Key Outputs

2.6.4.1. Threat led strategic requirement defined as input for risk management.
2.6.4.2. Mature the Cyber Controls Library and maintain measurements of control effectiveness.
2.6.4.3. Strategy for third-party cyber risk management, associated policies and procedures.

2.7. WP7: Maturing the Risk Management Framework.

2.7.1. The GRC RMF is required to be managed by allocated resource from the development and embedding stage into the operational and tactical areas where the outcomes of the entire project is successfully managed to a point where it is second nature to the programme and portfolio leads across the HO.
2.7.2. It is assessed that a profile and resource of a team of 4 – 5 personnel after 6 months being phased in throughout the year where the requirement is identified. They will be required to deliver the process to enhance the risk reporting, quality assurance, compliance and exceptions management within the GRC RMF. There will also be a requirement to generate summary level information on risk for high level boards and implementing the QA processes already developed eventually transitioning report generation to the automation tooling (ServiceNow).

2.7.3. Key Outputs

2.7.3.1. Facilitation of temporal Risk Management in accordance with the various policies.
2.7.3.2. Coaching the business areas on the RMF utility.

2.7.3.3. Leading the procedural changes in the RMF within the business areas.
2.7.3.4. Utilising the Automation toolsets.
2.7.3.5. Feeding additional requirements into the transformation programme as identified during their activities.
2.7.3.6. Maintain the criteria supporting the Risk Assessment process.
2.7.3.7. Reporting on metrics associated with Key Risk Indicators (KRI) and Key Performance Indicators (KPI).

2.8. WP8: Develop Cyber Risk data model and Reporting Capabilities (ServiceNow)

2.8.1. This workstream is intended to deliver a data model that provides outputs in support of a focused presentation of information to cyber risk management stakeholders.

2.8.2. The delivery partner is expected to identify and design an enhanced Management Information capability providing management with key metrics to steer decision making in support of managing cyber risk. Aligned to identified business criticalities, present threat-driven information on Cyber risk.

2.8.3. The delivery partner is required to develop Key Performance Indicators and Key Risk Indicators through determining appropriate metrics, establishing a baseline and delivering a business as usual capability to measure, capture, analyse and report.

2.8.4. The delivery partner is expected to embed the data model and reporting capabilities in ServiceNow

2.8.5. Key Outputs:

2.8.5.1. MI Enhancement Strategy.
2.8.5.2. Defined KPIs, risk analytics including KRIs.
2.8.5.3. Validation of risk metrics.
2.8.5.4. Implementation of measurement and recording capabilities.
2.8.5.5. MI report templates.
2.8.5.6. MI implemented in reporting tools.

3. KEY MILESTONES AND DELIVERABLES

3.1. The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date
Kick off meeting	Meeting to discuss the work packages and approach to be taken for the duration of the requirement to establish the project plan.	T0
WP1: Embedding plan and roadmap	Detail the next steps (at the conclusion of the scope of this SOR) for embedding the Risk Management Framework in Home Office and roadmap to show the timelines.	T0+24 months
WP1: Adoption report documenting adoption progress and including lessons learned.	Demonstrate the adoption of the framework and achieved risk reduction across Home Office. Capture experiences to enable effective future planning aimed at ALBs.	T0+12 months
WP1: Strategy to measure the effectiveness of the Framework in reducing cyber risk.	Develop the measurement criteria aligned to the adoption programme to enable tactical enhancements to the framework and associated processes to improve risk reduction.	T0 + 3 months
WP1: Effectiveness metrics report	A report detailing the effectiveness of the framework on cyber risk reduction across the home office.	T0 + 12 months
WP2: Cyber Risk Culture Assessment report	Report detailing the results of the cyber risk culture analysis and defining a set of initiatives to improve cyber risk culture and metrics to track.	T0 + 6 months
WP2: Training Plan for Skills Development	A detailed Training plan that develops the Cyber Risk culture across the HO	T0 + 4 months
WP2: Roadmap for Home Office Board Exercising	ExCo level engagement in cyber related exercises to achieve targeted initiatives to improve response to major incidents.	T0 + 6 months
WP2: Strategy for identifying and resolving non-standard cyber issues.	Design and pilot an approach to enable identification, assessment and treatment of cyber issues that are typically considered edge cases of Cyber risk.	T0 + 14 months

Milestone/Deliverable	Description	Timeframe or Delivery Date
WP3: Operating Model Effectiveness assessment	A review of the performance against the defined operating model and using outcomes to design improvements.	T0 + 12 months
WP4: A framework for ALB and ecosystem cyber risk management	Understand and deploy the framework to the wider Home Office ecosystem drawing on experience from embedding the Cyber Risk Framework within Home Office.	T0 + 9 months
WP4: Strategy and Road Map for ALB CRM	Outline the approach to influencing cross-government adoption of good cyber risk management.	T0 + 11 months
WP5: Plan for future tooling and automation enhancements.	This is intended to shape the planning for future tooling and automation activities. It should be driven by the progress achieved by the implementation partner in support of delivering the requirements defined in WP5.	T0 + 1 month
WP5: Phased delivery approach to the ServiceNow capability defined in the risk framework, delivered in multiple releases throughout the project	Increasing capability of the ServiceNow IRM Advanced Risk Capability. Anticipated to include design workshops for requirements articulation, development of user stories.	T0 + 12 months
WP5: Construct the technical architecture of ServiceNow ready for deployment	Develop the ServiceNow capabilities required for Cyber Risk Management.	T0 + 12 months
WP6: Strategy for third-party cyber risk management, associated policies and procedures.	Develop a strategy for third party cyber risk management aligned to the HO Cyber risk management framework.	T0 + 12 months
WP7: Reporting on metrics associated with Key Risk Indicators (KRI) and Key Performance Indicators (KPI).	Deliver reporting on KRI and KPI for consumption by governance boards, articulating strategic risk and risk trends.	T0 + 12 months
WP8: Defined KPIs, risk analytics including KRIs implemented in ServiceNow.	Using the measurement strategies defined in WP1, define the data model in ServiceNow and implement the reporting required for KPIs and KRIs.	T0 + 8 months
Close Down Review Meeting	This is to review the key outputs and deliverables against the	T0+24 months

Milestone/Deliverable	Description	Timeframe or Delivery Date
	requirement to identify any gaps that remain.	

3.2. Regular meetings are to be conducted in accordance with the targets stated below:

3.2.1. WP Kick off meetings.
3.2.2. Regular update meetings.
3.2.3. End of WP review
3.2.4. WP output reviews
3.2.5. As required by the Senior Leadership Team.

4. MANAGEMENT INFORMATION/REPORTING

4.1. Regular work package reporting will be conducted on a dynamic sprint basis where the team will report workstream kick-off, mid sprint and end of sprint updates with HOCS GRC G6.

4.2. Additional project oversight will be reported to the PMO function on a monthly basis where progress, Issues, risks and blockers will be discussed.

5. CONTINUOUS IMPROVEMENT

5.1. The buyer expects the supplier to continually improve the delivered services throughout the Contract duration.

5.2. The supplier should present new ways of working to the Authority during monthly/quarterly contract review meetings.

5.3. Changes to service delivery must be brought to the Authority's attention and agreed upon before implementation.

6. QUALITY

6.1. Quality assurance will be conducted iteratively throughout the project with regular check points and update sessions focusing on the quality of the output. This will align to ISO 9001 Quality Management Standards.

ANNEX B

Crown Commercial Service

[redacted]

QUESTIONNAIRE AND RESPONSE

CONTENTS

FURTHER COMPETITION QUESTIONNAIRE

- **INTRODUCTION**

1. This section sets out the questions that will be evaluated as part of this Further Competition.
2. The following information has been provided in relation to each question (where applicable):
    1. Weighting – highlights the relative importance of the question.
    2. Guidance – sets out information for the Potential Supplier to consider when preparing their response; and
    3. Marking Scheme – details the marks available to evaluators during evaluation.

- **DOCUMENT COMPLETION**

1. Potential Suppliers **must** provide a response to every question in the blue shaded boxes. All responses must be in Arial font, no less than size 11.
2. Potential Suppliers **must not** alter / amend the document in any way.
3. Potential Suppliers **must not** submit any additional information with your Tender other than that specifically requested in this document.

- **SCORING SUMMARY**

STAGE	QUESTION NUMBER	QUESTION	TOTAL SCORE AVAILABLE
1	[1]	Company Information	Information Only
	[2]	Potential Supplier Contact	Information Only
	[3]	Mandatory Questions (3.1)	Pass / Fail
2	[4]	Technical Question 4.1 – 15% Question 4.2 – 15% Question 4.3 – 5% Question 4.4 – 10% Question 4.5 – 10% Question 4.6 – 5%	**60%**

STAGE	QUESTION NUMBER	QUESTION	TOTAL SCORE AVAILABLE
	[5]	Social Value Theme 2 Tackling economic Inequality (5%) Theme 5 - Wellbeing (5%)	10%
3	[6]	Price	30%
		Total	[100%]

Statement of Works SOW000
Call-Off Contract Ref: **Project_18370(P_9660)**

Statement of Works

TN1. STATEMENT OF WORK ("SOW") DETAILS	
Upon execution, this SOW forms part of the Call-Off Contract (reference below). 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 Contact. 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.	
SOW Reference:	
SOW Title:	
SOW Version:	
SOW Status:	
Date of SOW:	
Call-Off Contract Reference:	
Variation Reference:	
Buyer Cost Centre Number:	
Estimated Cost	
Contingency:	
Pricing Model:	
Supplier:	
SOW Start Date:	
SOW End Date:	
Duration of SOW:	
PO Reference Number (if known):	

2. BUYER ENDORSEMENTS		
Role	Name	Dated
Business (Programme)		Click or tap to enter a date.
Business (Op. Cont. Mgr)		Click or tap to enter a date.
Commercial		Click or tap to enter a date.
Finance		Click or tap to enter a date.
Legal (if needed)		Click or tap to enter a date.
IR35 Sign-Off (if needed)		Click or tap to enter a date.

3. SOW CONTRACT SPECIFICATION - PROGRAMME CONTEXT	
Introduction	
Services	**Scope of the Contract** .
SOW Background	
Delivery phase(s)	☐ Discovery ☐ Alpha ☐ Private Beta ☐ Public Beta ☐ Live ☐ Retirement ☒ Other – Transition and Mobilisation services
Overview of Requirement	

4. WAYS OF WORKING, SUPPORT AND SERVICE LEVELS	
Ways of Working	
Location/s	The Services outlined within this SOW will be delivered to/from: Location — To 2 Marsham Street, London SW1P 4DF ☐ Lunar House, Croydon, CR9 2BY ☐ Soapworks. Colgate Ln, Salford M5 3LZ ☐ Alternate/Offsite working locations as applicable* ☐ This may include other Home Office locations Supplier's own premises ☐ Remote (home) working ☐ Offshore roles may be permitted under this Statement of Work

5. HIGH LEVEL INDICATIVE HMRC IR35 DETERMINATION
(Note that this is indicative. A full Buyer **SDOPQ** determination will still be needed)

No	Statement	Mark
1.	The Buyer is requesting named individuals for the role/s and/or will not accept substitutes for the key individual/s; and/or	☐
2.	The individual/s and or role/s will **not** be working to pre-agreed deliverable/increment milestones/service level agreements. e.g. they will be being directed as part of an integrated Buyer or Buyer appointed team (rainbow / blended); and/or	☐
3.	The Buyer requires flexibility to quickly redeploy the individual/s and/or role/s for purposes other than agreed outcomes as priorities change; and/or	☐
4.	The individual/s and/or role/s is/are being paid on a pure time and materials basis and are not carrying any financial risk to rectify/complete any agreed deliverables within the pre-agreed price; and/or	☐
5.	The individual/s and/or role/s will require to manage resources (governance, financial, systems, or people) within the Buyer's organisation or for organisations other than their own (e.g. an officer of the company); and/or	☐
6.	Other than mandatory training, the individual/s and/or role/s will require training by the Buyer in order to enable them to carry out their role/s.	☐

For the purposes of HMRC IR35, for the individual/s and/or role/s covered by this determination (*strike out **A**, **B**, or **C** as appropriate e.g.~~struck out~~* leaving one box clear):

~~A~~. The individual/s and/or role/s is/are deemed to be **inside the scope of HMRC IR35** based on the checked criteria identified above (inside if any have been checked). As such it is required that the individuals pay full PAYE/NI for the work undertaken and therefore must not be working for a Personal Services Company (PSC) unless via an approved umbrella organisation. The individual/s must not be a material shareholder (over 5%) within the organisation being contracted with

B. None of the above criteria have been checked and the work consists of clearly defined deliverables which must be completed within the fixed / capped time and material budget agreed for the work ahead of execution and the individual/s and/or role/s, from the perspective of the Buyer, are therefore **clearly fully outside the scope of HMRC IR35**

C. *None of the criteria has been checked, but there is a degree of uncertainty and therefore a full HMRC CEST determination certificate is attached for each individual.*

6. *The full HMRC CEST certificate states that the individual/s and/or role/s are **unambiguously outside the scope of HMRC IR35**.*
7. *The full HMRC CEST determination is indeterminate or inside IR35 and the individual/s and/or role/s is/are considered to be **within the scope of HMRC IR35.** Such individual/s are required to pay full PAYE/NI contributions via appropriate employment / umbrella cover. Individuals shall not have a material share holding.*

6. BUYER REQUIREMENTS – SOW DELIVERABLES

7. BUYER REQUIREMENTS – ADDITIONAL SOW SPECIFIC REQUIREMENTS

Delivery Plan

Indicative milestones are included in the table below:

ID	Milestone Name	Work Pkg	Description	Completion Trigger	Date	Char
1						
2						
3						
4						
5						

SOW Specific Transition and/or Implementation Plan Details

Dependencies

Assumptions

Responsibility Matrix

Assurance Roles

Activity

(Responsible, Accountable, Consult, Inform)

Buyer

Customer of individual service

Supplier

7. BUYER REQUIREMENTS – ADDITIONAL SOW SPECIFIC REQUIREMENTS

Key Sub-Contractors

Sub-Contractor	Role
N/A	

Who the Supplier will work with (report to)

Accountable Buyer Manager
The primary individual within the Buyer to whom the Supplier shall ultimately report to is:
Alternative Buyer Manager
In the absence of the primary individual, the alternate Buyer reporting individual shall be:

Engagement with the Buyer / Governance

N/A

Key Roles and Key Staff (Buyer)

Key Role	Key Staff Name (email)

Key Roles and Key Staff (Supplier)

Key Role	Key Staff Name (email)

7. BUYER REQUIREMENTS – ADDITIONAL SOW SPECIFIC REQUIREMENTS

Security Applicable to SOW

One or more parts of the scope of this Statement of Work may be required to be undertaken in Buyer approved secure locations
With individually approved Waivers, the Supplier is permitted to perform limited work in connection with this SoW.

SoW specific security requirements include:

The Supplier will not make available or provide any Supplier Background IPRs or Third Party IPRs as part of the Deliverables unless otherwise agreed below:

One or more Deliverables under this Statement of Work will contain Supplier Background and/or Third Party IPR and this shall be provided under the terms referenced below

The specific IPR (and associated licence terms) are detailed in:

Unless explicitly noted in this section this SoW shall be covered by the arrangements as detailed within the Contract.

This Statement of Work requires specific Data Processing arrangements

The specific data arrangements are held in the document entitled:

7. BUYER REQUIREMENTS – ADDITIONAL SOW SPECIFIC REQUIREMENTS

Standards Applicable to SOW

Standard	Version	Dated
N/A		Click or tap to a date. Click or tap to a date.

Statement of Work Specific Contract Management Requirements

8. RESOURCE PROFILE

Organisation

Resource Plan

Overtime

N/A

Time-sheeting

Time-sheeting is required for this Statement of Work	☐
Time-sheeting is NOT for charging purposes. Time-sheeting is purely for assurance and information purposes (e.g. understanding the actual versus charged for cost of service)	☐

Resourcing

8. RESOURCE PROFILE

9. CHARGES

Statement of Work Charges

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

Capped Time and Materials	Firm Price	Time and Material

Payment for Delivery

Financial Model

Reimbursable Expenses

Buyer's Right to Accelerate, Pause or Cancel Delivery (Partially or in Total)

10. VARIATIONS TO TERMS

Contract Schedule	Clause	Variation

11. SIGNATURES AND APPROVALS

10. VARIATIONS TO TERMS

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

For and on behalf of the Supplier:	
Name	
Title	
Signature	
Date	

For and on behalf of the Buyer:	
Name	
Title	
Signature	
Date	

Signed by an authorised signatory for and on behalf of the Secretary of State for the Home Department (known as Home Office) (the '**Buyer**')