DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

RM6187 Framework Schedule 6 (Order Form and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	Project 9809
THE BUYER:	The Secretary of State for the Home Department.
BUYER ADDRESS	2 Marsham Street, London, SW1P 4DF
THE SUPPLIER:	Bain & Company, Inc. United Kingdom
SUPPLIER ADDRESS:	40 Strand, London WC2N 5RW
REGISTRATION NUMBER:	FC014328.
DUNS NUMBER:	398713453
SID4GOV ID:	N/A

Applicable framework contract
This Order Form is for the provision of the Call-Off Deliverables and dated 5th July 2024.

It's issued under the Framework Contract with the reference number RM6187 for the provision of a Strategic Review of Home Office's DDaT function.

CALL-OFF LOT: Lot 2 Strategy and Policy

Call-off incorporated terms
The following documents are incorporated into this Call-Off Contract.
Where schedules are missing, those schedules are not part of the agreement and can not be used. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6187
3. The following Schedules in equal order of precedence:

Joint Schedules for RM6187 Management Consultancy Framework Three

- Joint Schedule 1 (Definitions)
- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

Call-Off Schedules

- Call-Off Schedule 1 (Transparency Reports)
- Call-Off Schedule 5 (Pricing Details)
- Call-Off Schedule 6 (ICT Services)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 9 (Security) Part A
- Call-Off Schedule 14 (Service Levels)

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility) – RM6187
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**.**

Supplier terms are not 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: 8th July 2024

Call-off expiry date: 30th September 2024

Call-off initial period: 3 months

Call-off Optional Extension Period: N/A

Call-off deliverables:
See Appendix A

Security
Short form security requirements apply – See Appendix B

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 are:
[redacted]

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

Call-off charges
Option A:

[redacted]

Please note that payment terms are as follows: Bain will invoice at the start of each full or partial month, with invoices to be paid within 30 days.

Reimbursable expenses
N/A

Payment method
The payment method for this Contract is BACS.

Buyer's invoice address

Home Office Shared Service Centre HO
Box 5015 Newport,
Gwent NP20 9BB
United Kingdom

hosupplierinvoices@homeoffice.gov.uk

Tel: 08450 100125 Fax: 01633 581514

FINANCIAL TRANSPARENCY OBJECTIVES
The Financial Transparency Objectives do not apply to this Call-Off Contract.

Buyer's authorised representative

[redacted]

Buyer's security policy

The Supplier shall comply with the relevant obligations under the HMG Security Policy Framework (Security policy framework - GOV.UK (www.gov.uk)

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

The Supplier warrants that it has ISO/IEC 27001:2013 certification for its Information Security Management and shall comply with and maintain such certification requirements.

The Supplier shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements.

The Supplier shall (when designing, procuring, implementing and delivering the Services) comply with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

The Supplier shall comply with the EU Code of Conduct on Data Centres' Energy Efficiency and any subsequent replacements. The Supplier shall ensure that any data centre used in delivering the Services are registered as a Participant under such Code of Conduct.

The Supplier shall comply with the Authority and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT Strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)" at https://www.gov.uk/government/publications/greening-government-ict-strategy.

Supplier's authorised representative

[redacted]

Supplier's contract manager

[redacted]

Progress report frequency

See Appendix A

Progress meeting frequency

See Appendix A

Key staff

[redacted]

Key subcontractor(s)

Not Applicable

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

Commercially sensitive information

1.1. In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2. Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3. Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

Appendix A hereof, on the basis that it represents Commercially Sensitive Information. Bain's capabilities, intellectual property, approaches, tools and experience are commercially sensitive and provide a competitive advantage. Bain's price point is a trade secret. The disclosure of such information would have a material and detrimental effect.

Service credits

Not applicable

Additional insurances

Not applicable

Guarantee

Not applicable

Buyer's environmental and social value policy

The Supplier shall, when working on the Sites, perform its obligations under this Call Off Contract in accordance with the Environmental Policy of the Customer.
The Customer shall provide a copy of its written Environmental Policy (if any) to the Supplier upon the Supplier's written request.

"Environmental Information Regulations or EIRs"	a) means to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Customer;
"Environmental Policy"	a) means the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such regulations;

Social value commitment

Not applicable

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

Formation of call off contract

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

[redacted]

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

Appendix B
Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

Definitions

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

"Breach of Security"	the occurrence of: any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and has been updated from time to time.

7. **Complying with security requirements and updates to them**

i. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

ii. The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

iii. Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

iv. If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables, it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

v. Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

8. Security Standards

i. The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

ii. The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

   i. is in accordance with the Law and this Contract;

   ii. as a minimum demonstrates Good Industry Practice;

   iii. meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

   iv. where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

iii. The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

iv. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

9. Security Management Plan

i. Introduction

   i. The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

ii. **Content of the Security Management Plan**

i. The Security Management Plan shall:

1. comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
2. identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
3. detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
4. be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
5. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;
6. set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
7. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

iii. **Development of the Security Management Plan**

i. Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

Management Plan.

ii. If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

iii. The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However, a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

iv. Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

iv. **Amendment of the Security Management Plan**

i. The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

1. emerging changes in Good Industry Practice;
2. any change or proposed change to the Deliverables and/or associated processes;
3. where necessary in accordance with paragraph 2.2, any change to the Security Policy;
4. any new perceived or changed security threats; and
5. any reasonable change in requirements requested by the Buyer.

ii. The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

1. suggested improvements to the effectiveness of the Security Management Plan;
2. updates to the risk assessments; and

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

3. suggested improvements in measuring the effectiveness of controls.

iii. Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

iv. The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

10. **Security breach**

i. Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

ii. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

i. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

1. minimise the extent of actual or potential harm caused by any Breach of Security;
2. remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
3. prevent an equivalent breach in the future exploiting the same cause failure; and
4. as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

iii. In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the

DocuSign Envelope ID: F05D6A88-2142-4903-A146-DC5C5BD1725B

Buyer.