# Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

1. **PURPOSE**
	1. The purpose of this document is to provide a statement of requirements for an NCSC-assured Cyber Security Consultancy provider to support the Cabinet Office’s Cyber Security function for the provision of Strategic Co-sourcing for surge capacity in Cyber, to be issued under the Framework Contract with the reference number RM6187 Lot number 2, Strategy and Policy for the provision of Strategic Co-sourcing for surge capacity in Cyber.
	2. This work must start no later than 1 January 2023.
2. **BACKGROUND TO THE CONTRACTING AUTHORITY**
	1. The Cabinet Office supports the Prime Minister and ensures the effective running of government. The Cabinet Office is also the corporate headquarters for government, in partnership with HM Treasury, and takes the lead in certain critical policy areas. The Cabinet Office has responsibility for:
		1. Supporting collective government, helping to ensure the effective development, coordination and implementation of policy
		2. Supporting the National Security Council and the Joint Intelligence Organisation, coordinating the government’s response to crises and managing the UK’s cyber security
		3. Promoting efficiency and reform across government through innovation, better procurement and project management, and by transforming the delivery of services
		4. Promoting the release of government data, and making the way government works more transparent
		5. Creating an exceptional Civil Service, improving its capability and effectiveness
		6. Political and constitutional reform
	2. The Cabinet Office’s Digital directorate is the department’s IT and digital shared services function.
	3. Cabinet Office Cyber Security sits within the Digital directorate. It is the internally-facing cyber security team for the Cabinet Office, with a mission to secure the Cabinet Office against cyber threats. It delivers on this mission through four core tasks:
		1. Defining the cyber security policies and standards that Cabinet Office services, teams and staff must meet
		2. Delivering the cyber security capabilities to services, teams and staff to help and support them to meet those policies and standards
		3. Assessment and reporting on compliance against cyber security policies and standards
		4. Enabling an effective and efficient cyber security function
3. **BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT**
	1. High calibre individuals to deliver work according to Schedule 20, who will work at the direction of the Buyer to support them with maturing their cyber defence capabilities, by providing security architecture and security engineering services
	2. All candidates to be minimum of BPSS security clearance. BPSS Certificate to be approved by the Buyers Security Dept PRIOR to working on this Call Off Contract.
4. **DEFINITIONS**

| **Expression or Acronym** | **Definition** |
| --- | --- |
| OGDs | means Other Government Departments |
| COO | means Chief Operating Officer, and in the case of the Cabinet Office is the senior civil servant responsible for leading the department’s Corporate Services Group |
| CDIO | means Chief Digital and Information Officer, and in the case of the Cabinet Office is the senior civil servant responsible for leading the department’s Digital Directorate |
| CISO | means Chief Information Security Officer, and in the case of the Cabinet Office is the senior civil servant responsible for leading the department’s Cyber Security function |
| CTO | means Chief Technology Officer, and in the case of the Cabinet Office is the senior civil servant responsible for leading the department’s Technology team |

1. **SCOPE OF REQUIREMENT**
	1. For the purposes of this requirement, all IT and digital services owned by the Cabinet Office (and its arms-length bodies) and operating at OFFICIAL are in-scope.
	2. For the avoidance of doubt, the “Cabinet Office” includes (but is not limited to): Government Functions & Services, Corporate Services, Union and Constitution Group, the Cabinet Secretary Group, Inquiries, the Economic and Domestic Secretariat, Number 10, the Prime Minister's Delivery Unit & Data Science, the Foreign Policy and National Security Secretariat, the Joint Intelligence Organisation, and the Government in Parliament Group.
	3. IT and digital services not owned by the Cabinet Office (i.e. owned by other government departments or commercial partners) are not in scope. IT and digital services processing SECRET or above are not in scope.
2. **THE REQUIREMENT**
	1. The individuals will be allocated a Buyer Line Manager who allocates workload and will have weekly ‘one to ones’ in order to assess performance and allocate work load/objectives accordingly.
	2. There will be a weekly contract management meeting with the Supplier Partner, and from the buyer the CO Contract Manager CDIO Head of Cyber Security and the CDIO DD Cyber for the first 4 weeks of the contract, which will reduce to a frequency to be jointly agreed.
		1. This will discuss work delivered to date and any future work planned by the supplier, any risks or issues, and any other business as agreed. Appropriate Management Information and reporting to be submitted by the supplier to the buyer no less than 24 hours prior to these meetings.
3. **KEY MILESTONES AND DELIVERABLES**

7.1 Progress meeting and report frequency deliverable

There will be a report provided weekly in respect to the contract management meeting. The frequency of which will be agreed by the Parties via the meeting.

7.2 The following Contract milestones shall apply:

| **Milestone** | **Description** | **Timeframe or Delivery Date** |
| --- | --- | --- |
| 1 | Contract Start Date | 1 January 2023 |
| 2 | Contract End Date | 31 March 2023 |

1. **MANAGEMENT INFORMATION/REPORTING**
	1. As recorded above under point 7.1
2. **VOLUMES**
	1. None noted.
3. **CONTINUOUS IMPROVEMENT**
	1. The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
	2. The Supplier should present new ways of working to the Authority during monthly/quarterly Contract review meetings.
	3. Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.
4. **SUSTAINABILITY**
	1. None noted.
5. **QUALITY**
	1. The Supplier will deliver the Services in a way that enables the Authority to comply with its obligations under the Technology Code of Practice, which is available at: https://www.gov.uk/government/publications/technology-code-of-
	practice/technology-code-of-practice.
	2. The quality standards required for this Call-Off Contract are ISO/IEC 27001, see Security Standards, and the Supplier shall maintain appropriate internal systems and processes to ensure the quality of service delivered under this agreement.
	3. All deliverables produced by the Supplier under the requirement will go through two cycles of review by the Authority. The final deliverables will be formally signed-off by the Authority’s designated representative.
6. **PRICE**
	1. The budget for this work is expected to be £160,000.00 excl VAT.
	2. The supplier shall provide a proposed fixed-fee price for the delivery of the requirement from 1 Jan 2023 to 31 Mar 2023.
	3. The Supplier shall provide the proposed fixed-fee price for the delivery of the requirement in response to an expression of interest (EOI) issued by the buyer. The Supplier shall also provide a daily rate card showing prices for agreed follow-on work.
7. **STAFF AND CUSTOMER SERVICE**
	1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
	2. The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
	3. The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.
8. **SERVICE LEVELS AND PERFORMANCE**
	1. The Authority will measure the quality of the Supplier’s delivery through ongoing review of activities and outputs against quality standards and the agreed plan, and through adherence to the agreed KPIs.
	2. In the event of early termination of the contract due to conditions as per 10.4 of the core terms the Supplier must return to the Authority any Authority equipment and or materials used or produced during the services.
9. **SECURITY AND CONFIDENTIALITY REQUIREMENTS**
	1. The Supplier shall ensure that all staff supporting the authority hold UK National Security Vetting to “Security Check” (SC) level.
	2. The Supplier shall maintain compliance with ISO 27001:2013 and ISO 27018:2014, or Cyber Essentials Plus, or equivalent, and shall also ensure that any third parties used by it in the course of the service provision and deemed critical to the service, shall adopt a systematic approach to managing information so that it remains secure.
	3. Any OFFICIAL-SENSITIVE information shall be shared on a need to know basis and made accessible to named team members with the appropriate UK National Security Vetting only.
10. **PAYMENT AND INVOICING**
	1. A purchase order will be raised once the Contract has been signed. The purchase order is a vehicle for payment and not a firm commitment of spend.
	2. Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
	3. The Supplier shall submit invoices by email to REDACTED TEXT under FOIA Section 43 Commercial Interests and follow the below criteria:
		1. The invoice must include the purchase order number.
		2. All invoices must be in PDF format attached directly to the email.
		3. Each invoice may only be provided in a single file, including all supporting documentation. Additional or separate supporting documentation should not be attached as a separate file.
		4. Multiple invoices can be attached to one email but each invoice must be in a separate PDF (with no additional supporting files as described above).
		5. Invoices must not be password protected.
		6. The total size of the email must not exceed 4MB.
11. **CONTRACT MANAGEMENT**
	1. The Supplier will facilitate monthly (or as otherwise agreed) contract review meetings with the Cabinet Office.
	2. Attendance at contract review meetings shall be at the Supplier’s own expense.
12. **LOCATION**
	1. The Services will be delivered to the Cabinet Office, 10 South Colonnade, London, E14 4PH