|  |  |
| --- | --- |
|  | CALL-OFF CONTRACT  Cyber Security Services 2 RM3764ii  PART A Order Form , Specific Terms and  PART B Schedules  PART C RM3764ii Standard (non-variable)Terms *(held online)* |

|  |  |
| --- | --- |
| Buyer Ref: | *00188819/CCIS17B53* |
| Date sent to supplier: | 08/09/2017 |
| Purchase Order Number: | TBA |

**This agreement is between:**

|  |
| --- |
| the “Buyer”  Government Digital Service, Cabinet Office  The Whitechapel Building 10 Whitechapel High Street Aldgate London E1 8QS |
| the “Supplier”  EntServ UK Limited part of the DXC Technologies Group  216926139  Royal Pavilion, Wellesley Road, Aldershot, Hampshire, United Kingdom, GU11 1PZ |
| Together the “Parties” |

**Service delivery contact details:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Buyer:** | **Name:** | REDACTED | |
| **Title:** | Security Product Owner |
| **Email:** | REDACTED |
| **Telephone:** | REDACTED |
| **Supplier:** | **Name:** | REDACTED |
| **Title:** | UKPS Sales |
| **Email:** | REDACTED |
| **Telephone:** | REDACTED |

PART A – ORDER FORM

This Order Form is issued in accordance with the Framework Agreement Cyber Security Services 2- RM3764ii and the Buyers mini competition tender.

The Contract is made up of:

* Part A – The Order Form (an overview of the services to be provided throughout the lifetime of the agreement) and the Specific Terms (which are specific to this Contract)
* Part B – Schedules (the Buyers requirements, the winning suppliers bid and the agreed work to be carried out) and;
* Part C – Standard RM3764ii Call-Off Terms and Conditions (which are non-variable)

The Supplier agrees to supply cyber security services specified below on and subject to the terms of this Contract.

The Buyer will complete the Order Form prior to the Contract award.

|  |  |
| --- | --- |
| **Call-Off Contract term:** | |
| 1. Commencement Date: | 15/09/2017 |
| 1. Length of Contract: | Up to 3 years |

|  |  |
| --- | --- |
| **Contract Charges and payment** | |
| 1. The method of payment for the Contract Charges (GPC or BACS): | BACS |
| 1. Invoice details |  |
| * 1. Where and how to send invoices | REDACTED |
| * 1. Who to send invoices to: | REDACTED |
| * 1. Invoice information required: *e.g. PO, Project* | Purchase Order |
| 1. Invoice Frequency | Monthly |
| 1. Contract Charges | Completed post award – Insert suppliers winning bid and maximum Contract Charges for the duration of the Contract |

|  |  |
| --- | --- |
| **Buyer contractual requirements:** | |
| 1. Services required: \* | For the supply of Security Consulting – Penetration Testing part of project ref: 00188819.  Please note extent of the services exclude hardware devices and/or software products. |
| 1. Delivery Location(s)/Premises: | Customer Premises in London and Farnborough |
| 1. Relevant convictions: | None |
| 1. Staff Vetting and Security Clearance: | Clearance not to exceed SC Security Clearance |
| 1. Local health and safety procedures: | As per the Cabinet Office Instruction |
| 1. Non-Disclosure requirements: | No NDA required |
| 1. Exit Planning: | Not Applicable. |
| 1. Security Requirements:   (including details of Security Policy and any additional Buyer security requirements) \*\* | Cabinet Office to supply if required |
| 1. Protection of Buyer Data: | Not Applicable |
| 1. Standards: | CESG CHECK |
| 1. Business Continuity and Disaster Recovery: | Not Required |
| 1. Insurance: | As per Clause 16 of the [framework agreement RM3764ii](https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii)  *Liability Insurance – minimum level of cover £5,000,000*  *Professional Indemnity – minimum level of cover £1,000,000* |

|  |  |
| --- | --- |
| **Additional and/or alternative clauses:** | |
| This section allows the Buyer to add supplemental requirements and additional terms to the Contract. These must be completed before the requirements are published. | |
| 1. Supplemental requirements in addition to the Call-Off Terms | None] | |
| 1. Buyer Specific Amendments to the Call-Off Terms   The table below lists the editable terms from the [RM3764ii Standard Call-Off Terms](https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii).  The number of days, value or other elements of these terms may be increased to suit the Buyer’s needs. They may not be decreased. When amending these terms, the Buyer must state whether it has been increased or not. | |
| |  |  |  | | --- | --- | --- | | **Clause** | **Heading** | **Minimum Contract term (cannot be reduced)** | | 4 | Warranties and Representations | Will remain 90 Working days from the date the Buyer accepts the release of work. | | 18 | 1. Supplier Assistance at Retendering | Will remain 10 Working days | | 24 | 1. Force Majeure | Will remain 15 consecutive Calendar Days | | 19 | 1. Changes co Contract | Will remain 5 Working Days | | 37 | 1. Dispute Resolution | Will remain that active efforts will be made to resolve within 10 working days | | 38 | 1. Liability | Will remain   * direct loss or damage to property - £1,000,000 in each Contract Year in which the default occurred or is occurring * £500,000 or a sum equal to 200% depending on the liability damage/loss or impact | | 39 | 1. Termination Events Material Breach | Will remain 15 consecutive Calendar Days | | |

**Further information:**

**\*\* Security Requirements Note:**

If the Buyer requires work to be carried out at the OFFICIAL-Sensitive status or above, the Parties agree to complete a Security Aspect Letter to accompany the contract award.  
  
The Buyer may choose to issue a specific Security Aspects Letter to determine the security of the work undertaken.

**What is a security aspects letter?**  
Find out more: <https://www.gov.uk/guidance/defence-equipment-and-support-principal-security-advisor#frequently-asked-questions>

|  |  |
| --- | --- |
| **Winning Supplier’s information:** | |
| 1. Suppliers commercially sensitive information | None |
| 1. Key Sub-Contractors | None |
| 1. Contract Charges |  |

£16,235.00

|  |
| --- |
| **Acknowledgment:** |

* By signing and returning this Call-Off Contract the Supplier agrees to enter into agreement to supply Cyber Security Services to the Buyer as described in Cyber Security Services 2 RM3764ii.
* The Parties acknowledge and agree that they have read the Call-Off Contract and RM3764ii Standard Call-Off Terms and by signing below, agree to be bound by this Contract.
* The Parties acknowledge and agree that this Contract shall be formed when the Buyer acknowledges the receipt of the signed copy from the Supplier within two (2) Working Days. Ref: [RM3764ii Call-Off Procedure](https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii))
* The Contract outlines the deliverables and expectations of the Parties. Order Form outlines any terms and conditions amended within the Call-Off Contract. The terms and conditions of the Call-Off Order Form will supersede those of [RM3764ii Standard Terms](https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii).

**SIGNED:**

|  |  |
| --- | --- |
| Supplier: | Buyer: |
| Name: | REDACTED | REDACTED |
| Title: | Director - UKPS | product owner - security |
| Signature: | 13/09/2017 | 19/09/2017 |

PART B – THE SCHEDULES

Remove all guidance when complete

**SCHEDULE 1 – SERVICES NEEDED**

The Government Property Agency (GPA), as part of its remit to drive savings across the government estate, is looking to establish a number of multi-departmental offices in strategic locations, to be called “Hubs”. Relocating civil and public servants from existing, often fragmented office locations, to modern, cross-departmental workplaces will make the most of emerging working practices, and technology is part of that drive.

This project relates to the establishment of a secure, managed Wired and Wireless LAN at a new Government Hub at 10 South Colonnade, Canary Wharf (10SC). This testing merely relates to the initial tactical solution on the 6th floor of the building and the connection back to the connectivity hub.

It involves the deployment of an Aruba Wired and Wireless environment, utilising Aruba Mobility Controllers as centralised points of network control and enforcement, secured using Aruba ClearPass and managed via Aruba AirWave.

This infrastructure is connected to a centralized Connectivity Hub at Crown Hosting at Cody Park to provide onward connectivity to the internet and departmental resources.

The 10SC Hub site once fully provisioned will serve 7,500 concurrent users, with potential growth to 10,000. Of note are:

* High availability with no single point of failure
* Wired and wireless access in all occupied areas
* “GovWiFi” network service for all users from any organisation, subject to authentication
* Multiple department- or organisation-specific secure customer networks available to authenticated users
* All users and devices sharing a common network infrastructure
* No network access for unauthenticated users or devices
* No interconnection between secure customer networks (including “GovWiFi”) inside a Hub
* Centralised services for all Hub sites provided from Connectivity Hub
* Hub WAN connections easily accommodate Moves, Adds and Changes in Connectivity Hub architecture

**LAN (initially 10SC 6th Floor only)**

* 1000BaseT (10/100/1000) connectivity for client devices (including Wireless APs)
* Client connectivity into 40 Secondary Equipment Rooms (SERs) on 10 floors over Cat6 cable
  + Only 4 SERs are in-scope, as the test scope is limited a single occupancy floor
* Each SER cabled to two Main Equipment Rooms (MERs) with OM3 fibre
* PoE for Wireless APs
* Nominal 2.8 Mbit/s minimum bandwidth per connected client device at maximum user density
* Client access ports to operate without manual provisioning
* Future capability for SmartRate client and AP connectivity

**ClearPass**

* Resilient design
* Load balanced authentication requests
* Support for RADIUS and TACACS+ network device admin authentication
* Support for EAP-TLS with OCSP and CRL revocation checking
* Support for MAC authentication
* Support for 802.1x.

A grey box approach to testing is required.

**ESSENTIAL SKILLS AND EXPERIENCE**

This test must be operated under the NCSC CHECK scheme, as such, an appropriate CHECK team must be formed, as per scheme requirements.  
  
Proposals **must** include, or be accompanied by, test team CVs. Where CVs of named test team members cannot be provided, indicative CVs should be.

The following certifications are requested and preferred wherever possible:

* CREST Certified Network Intrusion Analyst
* CREST Certified Wireless Specialist
* CREST Certified Infrastructure Tester

While CREST certifications mentioned are preferred, a tester with demonstrable experience within a correctly formed CHECK team would be considered. A single person may be certified to the requested levels.  
  
Possession of the ISO 9001 certification would be beneficial, however is not a specific requirement for this assignment.  
  
The test team should show prior experience of specific skills in submitted CVs for:

* 802.1x equipment
* Networking equipment
  + Cisco and HPE Aruba are very strongly preferred

**SCHEDULE 2 - HIGH LEVEL DELIVERY PLAN**

The DXC Penetration Testing team engagements are all led by CHECK qualified Team Leaders. This individual will be your single point of contact on site during the delivery of the test. The Team Leader will work with you to ensure all aspects of testing are covered and completed in a timely manner.

Testing @10SC Office London

* Wireless penetration testing
* Configuration review of
  + 2 x Core Switches 5940
  + 4 x Access Switches 5412
  + 2 x Aruba 7220 Local Controllers
* Segregation test / Exposure review

Testing @Cody Park

* Infrastructure test and build review of the following servers
  + 3 x ClearPass servers
  + 2 x Mobility Master Servers
  + 1 x AirWave
  + 1 x Syslog Server
* Device configuration review of the following switches
  + 2 x Cisco 93180YC Switches running NXOS
* Firewall configuration review of the following firewalls
  + 1 x Cisco ASA 5525
  + 2 x Cisco Firepower 4110 ASA

The team structure and estimated person-days is:

1 day workshop (CTL)

5 days testing London (3CTL days + 2 CTM days)

4 days testing Farnborough (2CTL days + 2 CTM Days)

3 days reporting (3 CTM days)

.

**SCHEDULE 3 - BUYER RESPONSIBILITIES**

Winning supplier to add any responsibilities of the Buyer here. Include anything that the Suppleir needs the Buyer to do, to enable them to do their job.

**SCHEDULE 4 – NON-DISCLOSURE AGREEMENT**

Not Required

**SCHEDULE 5 – STATEMENT OF WORK (SoW)**

**Overview:**

The testing requirement will comprise of:

**Workshop (Pre-test briefing)**On on-site workshop is required prior to the start of testing phase(s) and should be attended by at least the CHECK Team Leader.

Additional architecture documentation will be shared after supplier selection and award, prior to the Workshop itself. The workshop is expected to be 1 day. The workshop phase must be on-site at 10SC (10 South Colonnade, Canary Wharf, London, E14 5AB).

Prior to the commencement of any phases, named tester information must be provided together with security clearance details to allow the creation of required authentication/access credentials. Such details should include full name; contact details; public SSH key(s) and source IP address information if off-site testing is opted for.

**Reporting**

Analysis; reporting and quality assurance phase(s) should take place from supplier remote offices’ and location(s).

One holistic report is expected, with a draft and/or interim release being made available as soon as possible after closing of testing, prior to any optional re-testing. The report shall be marked OFFICIAL-SENSITIVE and handled accordingly.   
  
The reports must include details on:

1. what was tested;
2. how it was tested;
3. steps to reproduce any problems found; what results were found; and
4. include what techniques and tools (including versions for COTS/Open Source tools) were used to carry out the test;
5. use the CVSS2 marking scheme;
6. clearly identify / number the vulnerabilities found for tracking purposes;
7. include an accompanying results summary in spreadsheet format.

At the end of each testing day of testing an informal update is required. This could take the form of a verbal update or a brief highlight email report listing the issues found.

**Re-testing**

Any re-testing, if required, would commence approximately five (5) working days after the production of formal report(s) or at a time to be agreed with the client.  
**Scope**

Please use the information provided in the following sections to determine the scope for the tests.

The ITHC will include, but not be limited to:

* Wired Network security & architecture test & review including, but not limited to:
  + segmentation testing between clients
  + segmentation testing between client and management
  + configuration and ‘build’ reviews of all devices; servers and services
  + firewall rule review(s)
* Denial of Service testing.

GDS wish to engage as follows:

I.T. Health Check / penetration testing, informed by the contents of this document, should include, but not be limited to, the following:

* Does the implementation successfully mitigate the perceived risks;
* Is it robust and efficient in the way it does so;
* Do any of the components fail standard network wired and wireless security tests;
* Does the configuration of each component meet best functional and security best practices;
* Supplier/tester expertise employed to provide further analysis both in technical implementation notes but also currently unforeseen risk and disclosure considerations;
* Other significant vulnerabilities.

Expected activities during the course of testing explicitly include (but are not limited to):

* device configuration and ‘build reviews’
* firewall rule reviews
* operating system & configuration ‘build reviews’

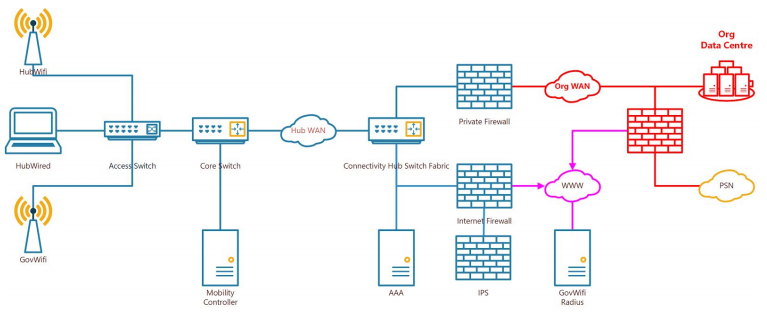
All testing should be conducted on-site, and based on components being tested will either be at 10SC (South Colonnade, Canary Wharf, London, E14 5AB) and/or Crown Hosting (Cody Park, Farnborough).

Re-test(s): Following the delivery of the report, GDS may require a follow-up meeting (virtual or face-to-face as appropriate) to discuss the findings and potential remedial actions.  
Once any remedial actions have been taken, GDS may request a retest of any significant identified vulnerabilities, aimed at verifying the effectiveness of the corrective actions taken.

## Scope - High Level Architecture

This section provides descriptive information about the system and should be used by bidders to help size their proposals.

This diagram shows a high level view of the functionality of the Hub.



Scope - Sizing Inputs

* Within the scope of testing @ 10SC will be the following devices:
  + 2 x Core Switches 5940
  + 4 x Access Switches 5412
  + 2 x Aruba 7220 Local Controllers
* Within the scope of testing @ Crown Hosting data centre at Cody Park:
  + 3 x ClearPass servers
  + 2 x Mobility Master Servers
  + 1 x AirWave
* The Connectivity Hub at Cody Park tactical solution is:
  + 2 x Cisco 93180YC Switches running NXOS
  + 2 x Cisco Firepower 4110 ASA
  + 1 x Cisco ASA 5525
  + 1 x Syslog Server.

**Principal Security Concerns**

* Whether the VLAN technology employed provides robust separation of tenants.
  + Consider this switch port to mobility controller, and between mobility controller and core switch. Subsequently to Connectivity Hub and Data Centre Network.
* Whether equipment is hardened in accordance with best industry practice and patching is up to date at the time of testing
* Whether wired interfaces are susceptible to attack.
* Whether management access and configuration is robust.
* Whether management and clients are adequately segregated.
* Whether clients are adequately segregated from each other.

|  |  |
| --- | --- |
| SoW start date: | 15/09/2017 |
| SoW Reference: |  |
| Buyer: |  |
| Supplier: | EntServ Uk Ltd  Royal Pavilion, Wellesley Road, Aldershot, GU11 1PZ |
| Sub-Contractors:  (list all sub-contractors) | None |
| Overall Estimated Service Completion Date:  (the “Completion Date”) | 22/12/2017 |
| Duration of SoW  (How long the SoW will last – expressed as Working Days) | 10 Working days |
| Charging Mechanism(s) for this SoW:  (Capped/ Time and Materials/ Time and Materials/ Fixed Price/ Milestone deliverables) | Fixed Price |

**Key Personnel:**

The Parties agree that the Key Personnel in respect of the Service Delivery are detailed in the table below.

**Table of Key Personnel:**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Details** |
| Phil Cheese | CHECK Team Member (CTM) | Attend workshop and London Tester |
| Luke Crowe | CHECK Team Lead (CTL) | Team Leader |
| Tom Bartlett | CHECK Team Member (CTM) | Farnborough Test |
|  |  |  |
|  |  |  |

**Deliverables:**

* Attend Scoping Workshop – 15/09/17
* CHECK Testing Activity at Cabinet Office Sites in London and Franborough
* Produce and deliver Test Report

**Additional Requirements**

Insert

**Balanced scorecard & KPIS:**

In addition to the Supplier’s performance management obligations set out in the framework agreement, the Buyer and the Supplier have agreed the following Balanced Scorecard & KPIs for this Release: (use this template and amend with your own measures in line with these headings) Copy of the below can be found [here](https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii)



**Contract Charges:**

The Maximum Price for this SoW is: £xxxxx

The preferred charging charging mechanism for this SoW is: (*Please tick below)*

|  |  |
| --- | --- |
|  | CAPPED TIME AND MATERIALS (complete Time and Materials table) |
|  | TIME AND MATERIALS (complete table below) |
|  | FIXED PRICE (complete table below) |
|  | MILESTONE DELIVERABLES |

The detail behind each charging mechanism is found below.

**Fixed Price**

* Where Services for this SoW are being delivered on a Fixed Price basis, the Contract Charges set out in the table below shall apply.
* The Parties acknowledge and agree that the following assumptions, representations shall apply in relation to the prices set out in the table below.
* Fixed Price Contract Charges (excluding VAT) shall be applied as follows:

| **Fixed Charge** | **Description** | **Service Period (or if Payment linked to Milestones then, Milestone Date)** | **Breakdown By Role and Duration** |
| --- | --- | --- | --- |
| £16,235.00 | CHECK Testing | 15/09/17 – 29/09/17 | Testers to attend CO London and Farnbourough and perform CHECK Testing and report findings. |
|  |  |  |  |
|  |  |  |  |

**Milestone Deliverables**

* Milestone Deliverable pricing shall be against the service delivery plan agreed by the Buyer and Supplier at the start of the SoW.
* The Supplier must complete the service Deliverable by the due date.
* The Buyer will review the Deliverable against the agreed acceptance criteria to sign off acceptance
* Once the Buyer has accepted the Deliverable the Supplier can raise and send an invoice.

**Agreement of SoW:**

By signing this SoW, the Parties agree to be bound by the RM3764ii Call-Off Contract terms and conditions set out herein:

**Signed by an authorised signatory for and on behalf of the Buyer and the Supplier**

**SIGNED:**

|  |  |
| --- | --- |
| Supplier: | Buyer: |
| Name: | REDACTED | REDACTED |
| Title: | director - ukps | product owner - security |
| Signature: | 13/09/2017 | 19/09/2017 |

Please send copies of all SoW to Crown Commercial Service email: [Cloud\_Digital@crowncommercial.gov.uk](mailto:Cloud_Digital@crowncommercial.gov.uk) titled Cyber Security Services 2 SoW.

**SCHEDULE 6 - CONTRACT CHANGE NOTE**

Call-Off Contract reference: Insert

Contract Change note variation number: Insert

**This amendment to the agreement is between:**

|  |
| --- |
| the “Buyer”  Buyer Full Name  Buyer Full Address |
| the “Supplier”  EntServ UK Ltd  216926139  Royal Pavilion, Wellesley Road, Aldershot, Hampshire, United Kingdom, GU11 1PZ (registered office address) |

**The variation:**

The Contract is varied as follows and shall take effect on the date signed by both Parties:

Full Details of the proposed change:

Insert

Reason for the change:

Insert

Likely impact, if any, of the change on other aspects of the Contract:

Insert

Words and expressions in this Contract Change Note shall have the meanings given to them in the Contract.

The Contract, including any previous changes shall remain effective and unaltered except as amended by this change.

**Signed by an authorised signatory for and on behalf of the Buyer and the Supplier**

**SIGNED:**

|  |  |
| --- | --- |
| Supplier: | Buyer: |
| Name: |  |  |
| Title: |  |  |
| Signature: | Microsoft Office Signature Line...  Select date | Microsoft Office Signature Line...  Select Data |

PART C – RM3764ii Standard Terms

The standard terms and conditions of the RM3764ii Call-Off Contract have been developed specifically for government/public sector.

These terms are non-variable and can be found on the CCS website:

<http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii>