Crown Commercial Service

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:	**CCSN19A27**
Date sent to supplier:	25/10/2019
Purchase Order Number:	TBC

This agreement is between:

the "Buyer"
Crown Commercial Service
REDACTED

the "Supplier"
NCC GROUP SECURITY SERVICES LIMITED
REDACTED

Together **the "Parties"**

Service delivery contact details:

Buyer:	**Name:**	REDACTED
	Title:	
	Email:	
	Telephone:	
Supplier:	**Name:**	REDACTED
	Title:	
	Email:	
	Telephone:	

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:**	28/10/2019
2.	**Length of Contract:**	*3 MONTHS WITH THE OPTION TO EXTEND 1 MONTH*

Contract Charges and payment

3.	**The method of payment for the Contract Charges** (GPC or BACS):	BACS
4.	**Invoice details**	
4.1.	Where and how to send invoices	REDACTED
4.2.	Who to send invoices to:	REDACTED
4.3.	Invoice information required: *e.g. PO, Project*	REDACTED
5.	**Invoice Frequency**	REDACTED
		£12,500.00

6. Contract Charges

Lot bidding for	Roles providing	Day rate*	T&S	Total	No. Of people	No. of Days	Total cost
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
							£ 12,500.00

Buyer contractual requirements:

7.	**Services required: ***	For the supply of 'IT Health Check' part of project ref: CCSO19A58. Please note extent of the services exclude hardware devices and/or software products.
8.	**Delivery Location(s)/Premises:**	To be completed by the Customer
9.	**Relevant convictions:**	N/A
10.	**Staff Vetting and Security Clearance:**	The Supplier must be able to provide staff with appropriate clearance. As a minimum staff should have or be willing to undergo the Baseline Personnel Security Standard (BPSS) although National Security Vetting clearance is preferable.
11.	**Local health and safety procedures:**	N/A
12.	**Non-Disclosure requirements:**	N/A
13.	**Exit Planning:**	As per Clause 11 of Framework RM3764ii terms and conditions.
14.	**Security Requirements:** (including details of Security Policy and any additional Buyer security requirements) **	As per Clause 21 of Framework RM3764ii terms and conditions.

15.	**Protection of Buyer Data:**	As per Clause 21 of Framework RM3764ii terms and conditions.
16.	**Standards:**	CESG Cyber Security Consultancy Standard
17.	**Business Continuity and Disaster Recovery:**	As per Clause 17 of Frameowrk Agreement RM3764ii
18.	**Insurance:**	REDACTED

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.

19. Supplemental requirements in addition to the Call-Off Terms N/A]

20. Buyer Specific Amendments to the Call-Off Terms

The table below lists the editable terms from the RM3764ii Standard Call-Off Terms.

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	Supplier Assistance at Retendering	Will remain 10 Working days
24	Force Majeure	Will remain 15 consecutive Calendar Days
19	Changes co Contract	Will remain 5 Working Days
37	Dispute Resolution	Will remain that active efforts will be made to resolve within 10 working days
38	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	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:

21. Suppliers commercially sensitive information	Winning supplier to confirm any commercially sensitive information from their bid.
22. Key Sub-Contractors	N/A

23. Contract Charges

Lot bidding for	Roles providing	Day rate*	T&S	Total	No. Of people	No. of Days	Total cost
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
							£ 12,500.00

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)
- 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.

SIGNED:

	Supplier:	**Buyer:**
Name:	REDACTED	REDACTED
Title:	REDACTED	REDACTED
Signature:	REDACTED	REDACTED

PART B – THE SCHEDULES

Remove all guidance when complete

SCHEDULE 1 – SERVICES NEEDED

Definitions

Expression or Acronym	Definition
AWS	Means Amazon Web Services
CCS	Means Crown Commercial Service
CHECK	Means the scheme under which NCSC-approved companies can conduct authorised penetration tests of public sector and CNI systems and networks.
ITHC	Means IT Health Check
DNS	Means Domain Name System
TLS	Means Transport Layer Security
VPC	Means Virtual Private Cloud

SCOPE OF REQUIREMENT

The requirement is to conduct an ITHC on the CCS Digital Travel Solution.
The CHECK scheme ITHC service provider will:

- Undertake testing to uncover vulnerabilities and bugs in the service;
- Provide a report documenting the ITHC and the vulnerabilities and bugs identified.
- Re-test any fixes that are implemented in response to the vulnerabilities and bugs identified.

The Requirement

This scope description is divided into a number of controls that have been selected from the overall control set as suitable for ITHC assurance testing. The scope description should not be seen as a constraint on the ITHC; it aims to focus attention on specific areas of the Digital Travel Solution implementation but should not constrain the test team from investigating other areas that may be of concern to the assurance activity.

Data in Transit Protection - All connections between Digital Travel Solution and its users (which include 'regular' users, admin staff from CCS and government Departments, suppliers to government Departments and Third Party Supplier staff) should be secured by a TLS implementation. Some access may also be provided by SSH for Third Party Supplier staff.
It should not be possible to connect to the service, irrespective of the user type, without the use of TLS or equivalent secure transport mechanism (eg SSH).

Where TLS is used the application must enforce the use of TLS 1.2:
– No ability to 'fall back' to an older version of the protocol;
– Suitable crypto suite with a minimum 128-bit AES (eg AES-GCM-128);
– Authentication by either RSA or EC-DSA using certificates from a tier 1 public CA using a minimum key size of 2048-bits (RSA) or 256-bits (EC-DSA);
– Implementation patched against known vulnerabilities.

Where SSH is used the application must enforce the use of SSH2:
– No ability to 'fall back' to an older version of the protocol;
– Suitable crypto suite with a minimum 128-bit AES (eg AES-GCM-128);
– Authentication by either RSA or EC-DSA using a minimum key size of 2048-bits (RSA) or 256-bits (EC-DSA);
Implementation patched against known vulnerabilities.

Supplier connections are B2B using an API:
– If TLS mutual authentication is used validate that only valid supplier certificates are accepted;

Digital Travel Solution acts as a managed portal that redirects users to supplier sites (depending on the user's Departmental affiliation).
– It should not be possible to be redirected to any non-HTTPS URL

Separation Between Users - In the context of a cloud service this refers to separation from other tenants of the shared service. It is planned that this separation be achieved on AWS using VPC.
Confirm that it is not possible to 'break out' or 'break in' to the VPC tenancy.
Confirm that all aspects of the service are contained within the VPC tenancy:
– Data is held within a relational database implemented on the AWS RDS platform;
– confirm that the required separation from other users is maintained.

Vulnerability Management - The service provider should provide a service to track vulnerabilities and install patches. This applies to the infrastructure (which is built on AWS IaaS) as well as the application.
Confirm that all operating system platforms, supporting applications (eg SQL Server) as well as the Digital Travel Solution application do not have any unpatched vulnerabilities;
- There should be no 'critical' or 'Important' (CVSS High, Medium) vulnerabilities present;
– There may be 'other' (CVSS Low) vulnerabilities present
– Comment on their impact.

Confirm that all operating system platforms are configured in accordance with relevant guidance (eg CIS Benchmarks).
Confirm that the underlying cloud services are configured in a secure manner.

Protective Monitoring - The service provider should provide a protective monitoring service to log all security-related events, audit these records and identify potential security incidents for investigation.

Confirm that events are logged:
– For all users of the service;
– Both success and failure of security-effecting events;
– Logged data should be adequate to describe the event.

Confirm that malicious use is logged, audited and detected (eg brute force login) Separation and Access Control within Management Interfaces.

Separation and Access Control within Management Interfaces

Confirm service management interfaces are isolated from any other service:
– There is no visibility of the service to any other user;

– Specific user roles (eg Department admin) are restricted to information they have a NTK;
– Only designated Third Party Supplier staff are able to change the operational status of the service;
– Only CCS staff are able to change the application configuration.

Functionality provided by a service management interface is limited to that needed to operate the service.
Identity and Authentication - All access to the Digital Travel Solution service (regular use, service management or operational) is required to authenticate using multi-factor authentication mechanisms. Note that the service (for regular users) also acts as an identity portal; SAML tokens with some user attributes are generated prior to redirection to a supplier site.
Confirm that is not possible to access the service (irrespective of user type) without providing at least two independent authentication credentials.
Confirm that SAML token data is signed and timestamped.
Digital Travel Solution Application - All DNS information relating to the service should be provided by the UK Public Sector DNS service.
Confirm the authoritative source of all DNS information is the UK Public Sector DNS.
The rate at which new accounts can be created on the system via the self-registration service should be limited to prevent bulk-registration attacks. Confirm that registration is rate limited.
Supplier reports uploaded to the service via the supplier API should be read-only. Confirm that CCS and Department admin users cannot modify uploaded reports.

KEY MILESTONES AND DELIVERABLES

Milestone/Deliverable	Description	Timeframe or Delivery Date
1	An ITHC testing schedule will be planned with the appointed CHECK ITHC service provider. ITHC and Penetration Testing shall be scoped to include testing of the service in the cloud.	Within 2 weeks of Contract Award
2	The CHECK scheme ITHC service provider will provide a report documenting the ITHC and the vulnerabilities and bugs identified.	Within 4 weeks of Contract Award

MANAGEMENT INFORMATION/Reporting

The Supplier will provide a report documenting the ITHC and the vulnerabilities and bugs identified.

Volumes

As stated in chapter 6 the requirement

Continuous Improvement

Not applicable.

Sustainability

Not applicable.

QUALITY

The IT Health Check will be performed by an approved tester who is part of the CHECK scheme and has relevant experience for the scope of the testing.
https://www.ncsc.gov.uk/information/using-check-provider
The Supplier must comply with the Digital Service Standard. https://www.gov.uk/service-manual/service-standard
The Supplier is to deliver the service in line with the Cloud Security Principles, the Security Design Principles and the Bulk Data guidance. https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

PRICE

The Supplier shall provide prices for each of the following activities:-
Testing to uncover vulnerabilities and bugs in the service;
Production of a report documenting the ITHC and the vulnerabilities and bugs identified: and
Re-testing any fixes that are implemented in response to the vulnerabilities and bugs identified.
Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

STAFF AND CUSTOMER SERVICE

The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

SERVICE LEVELS AND PERFORMANCE

Not applicable

SECURITY AND CONFIDENTIALITY REQUIREMENTS

IT Health Check will be performed by an approved tester who is part of the CHECK scheme and has relevant experience for the scope of the testing.

PAYMENT AND INVOICING

The payment method is BACS.
Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs, together with the purchase order number and Call-Off reference.
Invoices should be submitted electronically to:
REDACTED
The payment profile for this Call-Off Contract is monthly in arrears.

CONTRACT MANAGEMENT

Not applicable

LOCATION

REDACTED
Travel may be required to any CCS offices to facilitate necessary meetings in the completion of the services.

Remote working and conferencing tools should be used where possible to maximize productivity and keep costs to a minimum.

SCHEDULE 2 - HIGH LEVEL DELIVERY PLAN

REDACTED

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

Optional to include at the Buyers discretion

N/A

SCHEDULE 4 – STATEMENT OF WORK (SoW)

This schedule outlines the work to be carried out within each delivery stage.

A new SoW needs to be created for each delivery package.

This is the order to the Supplier and is used to monitor and measure the delivery of the requirements. It is also used to cross reference invoicing against delivery.

The rights, obligations and details agreed and set out in each SoW, only apply to the Services and Deliverables for this SoW. They do not relate to any past or future SoW, unless specified.

Where applicable, the Buyer and the Supplier may also choose to add the following documents to complement this SoW:

- The initial Service Delivery Plan – developed for this SoW
- Addition documents to support the deliverables
- High level objectives for this SoW

Overview:

SoW start date:	29/10/2019
SoW Reference:	CCSO1958
Buyer:	Crown Commercial Service
Supplier:	NCC GROUP SECURITY SERVICES LIMITED
Sub-Contractors: *(list all sub-contractors)*	
Overall Estimated Service Completion Date: *(the "Completion Date")*	25/01/2020

Duration of SoW *(How long the SoW will last – expressed as 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
REDACTED	***REDACTED***	***REDACTED***
REDACTED	***REDACTED***	***REDACTED***
REDACTED	***REDACTED***	***REDACTED***

Deliverables:

- Enter Deliverables.

Additional Requirements

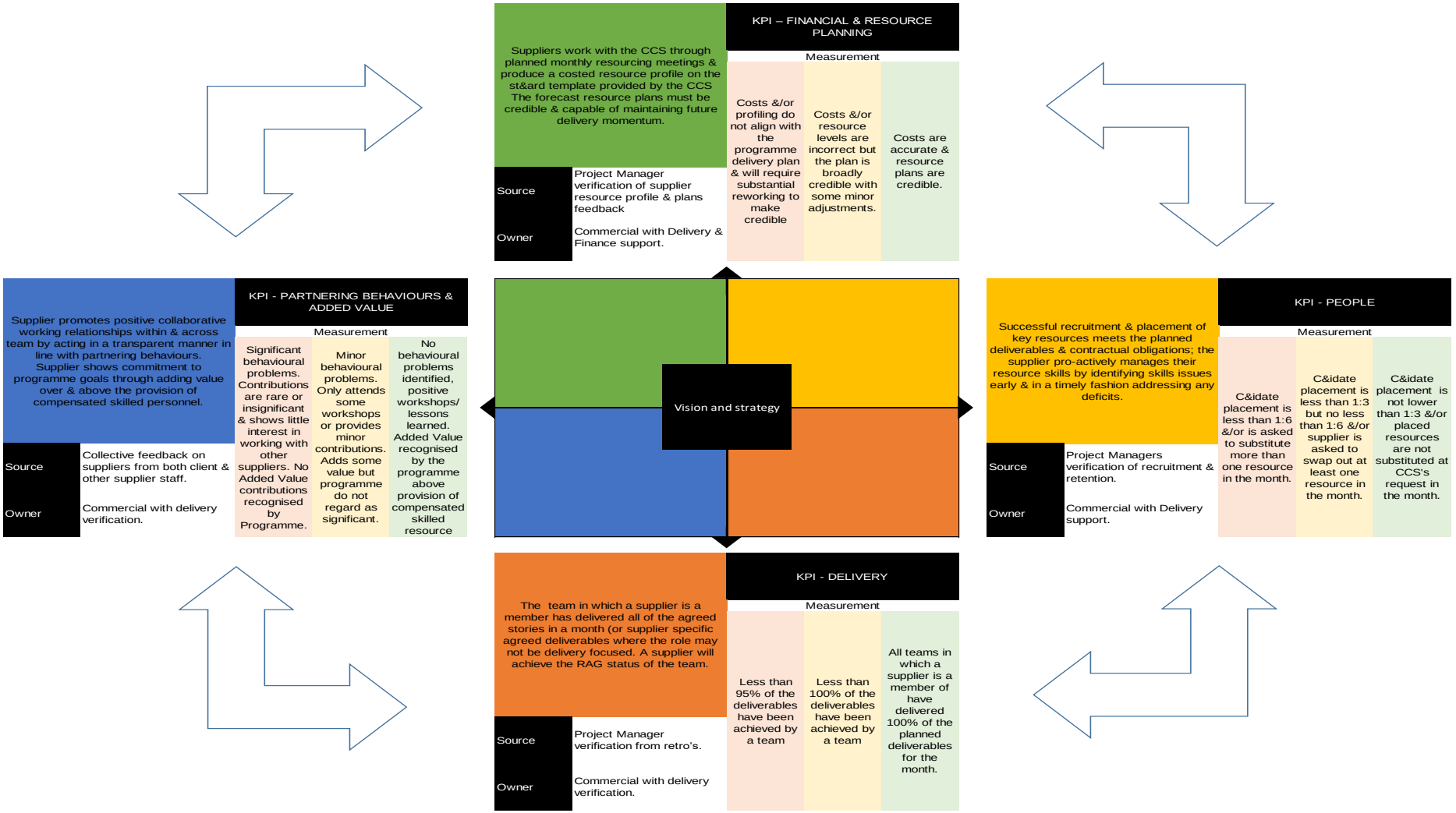
1.PURPOSE
1.1.The requirement is for an IT Health Check to be conducted on the CCS Digital Travel Solution service by a CHECK scheme ITHC service provider.

2.BACKGROUND TO THE CONTRACTING AUTHORITY
2.1.Crown Commercial Service (CCS) is a trading fund and Executive Agency of the Cabinet Office. We provide commercial and procurement expertise and services to government and the wider public sector (local authorities, NHS, police, education providers, devolved administrations).

3.BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT
3.1.An IT Health Check is required on an annual basis for this service to ensure vulnerabilities are identified and remediated.
3.2.Public sector customers of the Digital Travel Solution include Central Government Departments who expect the IT Health Check to be conducted annually. The eventual report(s) will be available to them on request.
3.3.Remote working and conferencing tools should be used where possible to maximize productivity and keep costs to a minimum.

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



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.

Capped Time and Materials

- The maximum price the Supplier is entitled to charge the Buyer for Services delivered on a Capped Time and Materials basis (excluding VAT but including Expenses) is known as the Maximum Contract Charges.
- The Buyer must specify if the Maximum Price for this SoW and stipulate the Service Period. E.g. Maximum Price per Week, per Working Days etc.
- Capped Time and Materials shall be calculated on a daily basis at the respective time and material rates for each Supplier Staff for every day, or pro rata for every part of a day, that the Supplier Staff are actively performing the Services and in accordance with the relevant rates for such Supplier Staff as required to perform such Services.
- The Supplier acknowledges and agrees that it shall provide the Services in relation to this SoW within the Maximum Price set out above; and it shall continue at its own cost and expense to provide the Services, even where the price of Services delivered to the Buyer on a Capped Time and Materials basis has exceeded the Maximum Price.
- The Buyer shall have no obligation or liability to pay for the cost of any Services delivered in respect of this SoW after the Maximum Price has been exceeded.

Time and Materials (T&M)

- The T&M pricing structure shall apply:
  - ✓ for Services delivered (or as agreed otherwise by the Parties); and
  - ✓ for other aspects of the Services as may be agreed by the Parties.
- T&M shall be calculated:
  - on a daily basis at the respective T&M rates for each Supplier Staff, for every day,
  - or pro rata for every part of a day that the Supplier Staff are actively performing the Services
- The relevant rates for such Supplier Staff is set out in the table below.
- The Supplier shall provide a detailed breakdown of any T&M; with sufficient detail to enable the Buyer to verify the accuracy of the T&M Contract Charges incurred.
- For the avoidance of doubt, no risks or contingencies shall be included in the Contract Charges in addition to the T&M.
- The Supplier shall retain a record timesheet for all staff providing the Services; which the Buyer may request for inspection at all reasonable times on request.
- T&M rates (excluding VAT) is an estimated cost for a SoW from Supplier proposal. If additional work is required. A further SoW is required. The Maximum Contract Charges may not be exceeded without consent from the Buyer. Please refer to Contract Change Note.

	Experience Level/ Day Rate/planned duration for this SoW						
Cyber Security Roles	Practioner Day Rate £	Planned Duration No. of Days	Senior Practioner Day Rate £	Planned Duration No. of Days	Lead Practioner Day Rate £	Planned Duration No. of Days	Total
Total value of this SoW:							
Estimated Contract Charge: *(23. of the Order Form)*							
Remainder of value under Estimated Contract Charge: *(23. of the Order Form minus All SoW total values)*							
Is there any risk to exceed Estimated Contract Charge: *Y/N & Comments below.*							Choose an item.
Comments:							

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:

Lot bidding for	Roles providing	Day rate*	T&S	Total	No. Of people	No. of Days	Total cost
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
							£ 12,500.00

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:		
Title:		
Signature:	X _____ Select date	X _____ Select Data

Please send copies of all SoW to Crown Commercial Service email: 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"

Supplier Full Name
Supplier No.
Supplier Full Address (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:	X _____ Select date	X _____ 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