



**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:	Security Testing IT - SR106703361
Date sent to supplier:	22/06/2018
Purchase Order Number:	AS PER STATEMENT OF WORKS

This agreement is between:

the “Buyer”

H M Revenue and Customs
5W Ralli Quays
3 Stanley Street
Salford
M60 9LA

the “Supplier”

BSI Cybersecurity and Information Resilience (UK) Ltd
6736691
389 Chiswick High Road, London, W4 4AL

Together the “Parties”

Service delivery contact details:

Buyer:	Name:	Redacted FOIA 2000 S41
	Title:	Redacted FOIA 2000 S41
	Email:	Redacted FOIA 2000 S41
	Telephone:	Redacted FOIA 2000 S41
Supplier:	Name:	Redacted FOIA 2000 S41
	Title:	Redacted FOIA 2000 S41
	Email:	Redacted FOIA 2000 S41
	Telephone:	Redacted FOIA 2000 S41

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:** [19/06/2018]
2. **Length of Contract:** 2 YEARS

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 FOIA 2000 S41]
 - 4.2. Who to send invoices to: [Should hard copy invoices be required these will be sent to:
Redacted FOIA 2000 S41]
 - 4.3. Invoice information required: *e.g. PO, Project* [All invoices must include purchase/limit order detail.]
5. **Invoice Frequency** [Invoice will be sent to the Buyer monthly]
6. **Contract Charges** [Redacted FOIA 2000 S43]

Buyer contractual requirements:

7. Services required: *

H M Revenue and Customs (HMRC) maintains an active and ongoing security programme of analysis of systems within the HMRC IT estate, and requires a CHECK approved provider to deliver a reliable, effective and proven service in order to support HMRCs ongoing security programme. This includes the following:

- Vulnerability Assessment
- Penetration Testing
- Health Checks

Additional services but not limited to:

- Internal Infrastructure Health Check
- Internal Penetration Test and Vulnerability Assessment;
- Security Assessment of workstations and laptops
- Firewall Configuration Assessment;
- Server Build Review;
- Android and iOS Mobile Device Review

Specifics of individual services will be defined on a case by case basis. Indicative estimates are that there will be 150 tests per year with 5 days and upwards needed for each test.

The Services will be delivered to multiple business areas within the Chief Digital Information Office across various locations. Each business area's requirements will be delivered under their own individual Statement of Works.

HMRC currently has reliance on one supplier to provide the above services. We would look to engage two further suppliers to fulfil the above indicative estimates. HMRC will manage the contract with the suppliers and will ask the suppliers to submit an Estimate based upon the scope of the Security Testing. The Estimate will be reviewed based upon timescales for completing work, availability of supplier's resources and location. This gives us the flexibility we require. Subcontracting and partnering is not permitted.

Additionally, they should be a National Cyber Security Centre (NCSC) approved security testing company with 2 or more CHECK team leaders.

8. Delivery Location(s)/Premises:	Various locations within the UK and possibly testing remotely
9. Relevant convictions:	Not applicable as all personnel engaged in the provision of this service to be at least SC cleared
10. Staff Vetting and Security Clearance:	All personnel engaged in the provision of this service to be at least SC cleared
11. Local health and safety procedures:	See supplemental requirements
12. Non-Disclosure requirements:	Not applicable
13. Exit Planning:	As Clause 11 of the Call-Off Contract Standard Terms
14. Security Requirements: (including details of Security Policy and any additional Buyer security requirements) **	See supplemental requirements 6.1 Buyer's Security Policy
15. Protection of Buyer Data:	All Buyer data/materials must be returned by the supplier
16. Standards:	ISO27001 Mandatory and ISO 9001 Desirable
17. Business Continuity and Disaster Recovery:	As per Call-Off Contract Standard Terms
18. Insurance:	As per Clause 16 of the framework agreement RM3764ii <i>Liability Insurance – minimum level of cover £5,000,000</i> <i>Professional Indemnity – minimum level of cover £1,000,000</i>

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	Within the scope of the Call-Off Contract, the Supplier will adhere to the following additional terms:
--	--

1 Purchase order mandatory policy

1.1 The Buyer operates a mandatory policy whereby official purchase orders will be issued in respect of all purchases made by the department. This ensures that every invoice received can be matched to a purchase order and to the corresponding goods or services received. Purchase orders will normally be issued from the Buyer's ERP system or, exceptionally, by any other procedure that has been specifically agreed in writing with the Buyer's Commercial

Directorate.

1.2 Any orders that are received by means other than those described in above are not authorized or sanctioned by the Buyer and should not be processed by suppliers.

1.3 The purchase order mandatory policy applies to the Buyer only.

2 Purchase order references

2.1 Suppliers should ensure that the relevant purchase order reference number is shown on all invoices and other ancillary documentation, such as delivery notes or order acknowledgements. Invoices must include the Buyer's purchase order number for them to be processed efficiently.

2.2 Failure to comply with the above requirement may result in invoices being returned to suppliers or payments delayed.

3 Payment of Invoices

3.1 The financial systems used by suppliers must be able to accept payment by the Bankers Automated Clearing Service (BACS).

4 Compliance with Value Added Tax and Other Tax Requirements

4.1 The Supplier shall at all times comply with the Value Added Tax Act 1994 and all other statutes relating to direct or indirect taxes

4.2 Failure to comply may constitute a material breach of this Call-Off Agreement and the Buyer may exercise the rights and provisions conferred by Clause 8.29 (Material breach termination) hereof.

4.3 The Supplier shall provide to the Buyer the name and, if applicable, the Value Added Tax registration number, PAYE collection number

and either the Corporation Tax or Self-Assessment reference of any agent, supplier or sub-contractor of the Supplier prior to the commencement of any work under this Call-Off Agreement by that agent, supplier or sub-contractor. Upon a reasonable request by the Buyer, the Supplier shall not directly assign a specific agent, supplier or sub-contractor as an account representative or dedicated support engineer or similar dedicated service role that Buyer requests not be so assigned.

5 SPATA

5.1 Where any personnel engaged in the provision of this contract is **liable** to be taxed in the UK in respect of consideration received under this contract, it shall at all times comply with the Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and all other statutes and regulations relating to income tax in respect of that consideration.

5.2 Where any personnel engaged in the provision of this contract is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall at all times comply with the Social Security Contributions and Benefits Act 1992 (SSCBA) and all other statutes and regulations relating to NICs in respect of that consideration.

5.3 The Buyer may, at any time during the term of this contract, request any personnel engaged in the provision of this contract to provide information which demonstrates how they comply with Clauses 5.1 and 5.2 above or why those Clauses do not apply to it.

5.4 A request under Clause 5.3 above may specify the information which any personnel engaged in the provision of this contract must provide and the period within which that information must be provided.

5.5 The Buyer may terminate this contract if-
(a) in the case of a request mentioned in Clause 5.3 above-

(i) any personnel engaged in the provision of this contract fails to provide information in response to the request within a reasonable time, or

(ii) any personnel engaged in the provision of this contract provides information which is inadequate to demonstrate either how they comply with Clauses 5.1 and 5.2 above or why those Clauses do not apply to it;

(b) in the case of a request mentioned in Clause 5.4 above, any personnel engaged in the provision of this contract fails to provide the specified information within the specified period, or

(c) it receives information which demonstrates that, at any time when Clauses 5.1 and 5.2 apply to any personnel engaged in the provision of this contract, they are not complying with those Clauses.

5.6 The Buyer may supply any information which it receives under Clause 5.3 to the Commissioners of Her Majesty's Revenue & Customs for the purpose of the collection and management of revenue for which they are responsible.

6 Buyer Specific Policies

6.1 The Supplier will comply with the Buyer's Security Policy



CSIR_Trusted Third
Party Access GPG V2_

6.2 The Supplier will comply with the Buyer's Health and Safety Requirements



HMRC Health and
Safety Policy.doc

6.3 The Supplier will comply with The Buyer's Behaviours Standards



Summary
Competency Framework

6.4 The Supplier will comply with the Buyer's Equality and Diversity Policy



HMRC diversity and
equality policy.doc

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	[REDACTED FOIA 2000 S43]
22. Key Sub-Contractors	[Sub-contractors not permitted]
23. Contract Charges	[Redacted FOIA 2000 S43]

[]

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:		
Title:		
Signature:		

PART B – THE SCHEDULES

SCHEDULE 1 – SERVICES NEEDED

H M Revenue and Customs (HMRC) maintains an active and ongoing security programme of analysis of systems within the HMRC IT estate, and requires a CHECK approved provider to deliver a reliable, effective and proven service in order to support HMRCs ongoing security programme. This includes the following:

- Vulnerability Assessment
- Penetration Testing
- Health Checks

Additional services but not limited to:

- Internal Infrastructure Health Check
- Internal Penetration Test and Vulnerability Assessment;
- Security Assessment of workstations and laptops
- Firewall Configuration Assessment;
- Server Build Review;
- Android and iOS Mobile Device Review

Specifics of individual services will be defined on a case by case basis. Indicative estimates are that there will be 150 tests per year with 5 days and upwards needed for each test.

The Services will be delivered to multiple business areas within the Chief Digital Information Office across various locations. Each business area's requirements will be delivered under their own individual Statement of Works.

HMRC currently has reliance on one supplier to provide the above services. We would look to engage two further suppliers to fulfil the above indicative estimates. HMRC will manage the contract with the suppliers and will ask the suppliers to submit an Estimate based upon the scope of the Security Testing. The Estimate will be reviewed based upon timescales for completing work, availability of supplier's resources and location. This gives us the flexibility we require. Subcontracting and partnering is not permitted.

Additionally, they should be a National Cyber Security Centre (NCSC) approved security testing company with 2 or more CHECK team leaders.

KPI's



SCHEDULE 2 - HIGH LEVEL DELIVERY PLAN

Not Applicable

SCHEDULE 3 - BUYER RESPONSIBILITIES

1 Assumptions

It is assumed that:

- Testing will be carried out using BSI secure testing laptops
- Reporting can be carried out remotely
- Work will be carried out in core office hours (09.00-17.00 Monday to Friday), unless otherwise agreed.

2 Dependencies

Dependent on HMRC and their stakeholders to:

- Provide appropriate approvals for the test to be carried out
- Carry out back-ups of systems prior to testing
- Provide testers with a place to carry out testing from, which comply with health and safety regulations
- Provide network schematics; URLs; and login accounts to support testing
- Ensure the system is operating and available for testing
- Confirm scope of testing prior to the commencement of testing
- Provide technical support throughout the testing
- Communicate any additional reporting requirements prior to the commencement of testing.

SCHEDULE 4 – NON-DISCLOSURE AGREEMENT

Not Applicable

Suppliers Tender Response

Redacted FOIA 2000 S43

Suppliers Supplementary Answers to Security Questions

Redacted FOIA 2000 S43

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:	[Select Date]
SoW Reference:	[]
Buyer:	[Buyer Full Name]
Supplier:	[Supplier Full Name]
Sub-Contractors: (list all sub-contractors)	[]
Overall Estimated Service Completion Date: (the "Completion Date")	[Select Date]
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)	Choose an item.

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
[]		

Deliverables:

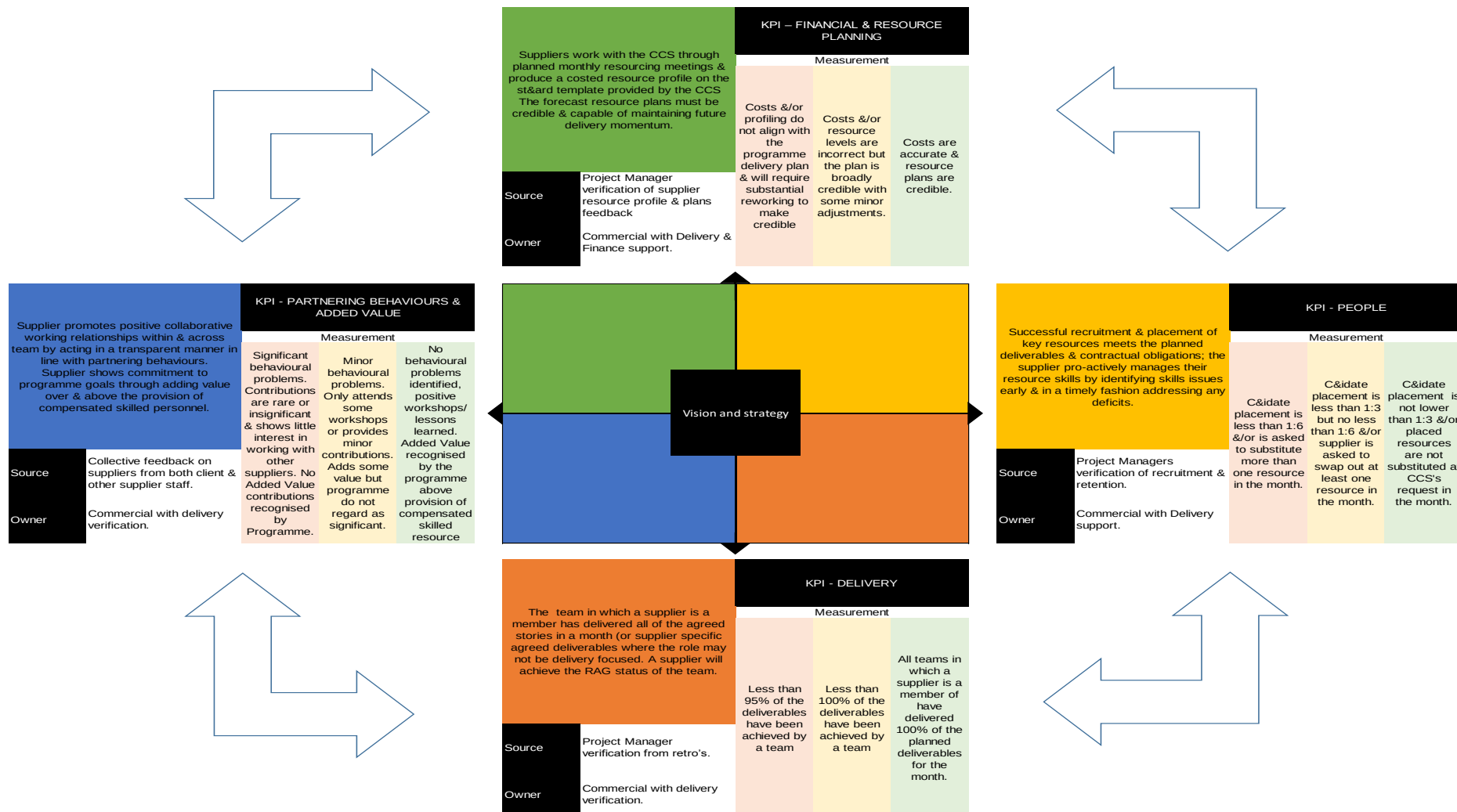
- Enter Deliverables.
- Enter Deliverables.
- Enter Deliverables.
- Enter Deliverables.
- Enter Deliverables.
- Enter Deliverables. |

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](#)



Contract Charges:

The Maximum Price for this SoW is: £xxxxx

The preferred 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:

Fixed Charge	Description	Service Period (or if Payment linked to Milestones then, Milestone Date)	Breakdown By Role and Duration
[]	[]	[]	[]
[]	[]	[]	[]
[]	[]	[]	[]

Milestone Deliverables

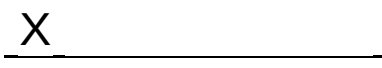
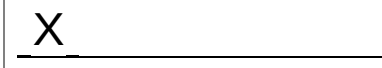
- Milestone Deliverable pricing shall be against the service delivery plan agreed by the Buyer and Supplier at the start of the SoW.
- The Supplier must complete the service Deliverable by the due date.
- The Buyer will review the Deliverable against the agreed acceptance criteria to sign off acceptance
- 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:		

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>