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:	*CCSN17A23*
Date sent to supplier:	15/12/2017
Purchase Order Number:	**TO BE COMPLETED POST TENDER**

This agreement is between:

the "Buyer"
Jamie Ryan
REDACTED
REDACTED
REDACTED
REDACTED
REDACTED
REDACTED

the "Supplier"
PwC
REDACTED

Together **the "Parties"**

Service delivery contact details:

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

	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:**	02/01/2018
2.	**Length of Contract:**	8 WEEKS

Contract Charges and payment

3.	**The method of payment for the Contract Charges** (GPC or BACS):	BACS
4.	**Invoice details**	Invoices MUST state a relevant Purchase Order Number and be sent to: REDACTED REDACTED REDACTED REDACTED
4.1.	Where and how to send invoices	PDF via email
4.2.	Who to send invoices to:	**REDACTED**
4.3.	Invoice information required: *e.g. PO, Project*	REDACTED
5.	**Invoice Frequency**	At Completion
6.	**Contract Charges**	£73,405.98

Buyer contractual requirements:

7.	**Services required: ***	For the supply of Cyber Security Research part of project ref: CCSN17A23. Please note extent of the services exclude hardware devices and/or software products.
8.	**Delivery Location(s)/Premises:**	REDACTED REDACTED REDACTED
9.	**Relevant convictions:**	N/A
10.	**Staff Vetting and Security Clearance:**	The Supplier must be able to handle and store classified material up to OFFICIAL level. The project report will be classified at OFFICIAL. Further information on security classification is available on the Cabinet Office website at the following addresses: • REDACTED • REDACTED
11.	**Local health and safety procedures:**	N/A
12.	**Non-Disclosure requirements:**	N/A
13.	**Exit Planning:**	The supplier should hand over the report and database as set out in Appendix B.
14.	**Security Requirements:** (including details of Security Policy and any additional Buyer security requirements) **	The Supplier will adhere to the following measures to keep this information secure. - The Supplier must ensure the security of the information in transit. - Any electronic files should be stored on an IT system that has access controls that only allow approved personnel with a genuine 'need to know' to access them to read and copy. The IT system should be protected by an appropriate firewall. - Once electronic files are no longer needed they should be deleted from the IT system in a way that makes recovery unlikely, either by overwriting the storage space or eventual dilution and deterioration on a busy shared storage system.

- Any electronic files or data should be stored within the UK.
- Paper copies (including drafts and notes) and any removable electronic storage must be locked away when not in use to prevent unauthorised access. Printed material should be marked OFFICIAL.
- Paper and printed material should be shredded when no longer needed.
- Access to all material generated by this project (not included source data unless supplied by DfT) must be on a limited and controlled basis, by persons notified to and approved by the DfT.
- The Supplier should have or be seeking to have Cyber Essentials certification. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
- Any personal information obtained under this contract must be controlled in compliance with the Data Protection Act

15.	**Protection of Buyer Data:**	As set out in point 14
16.	**Standards:**	CESG Cyber Security Consultancy Standard
17.	**Business Continuity and Disaster Recovery:**	N/A
18.	**Insurance:**	As per Clause 16 of the framework agreement RM3764ii *Liability Insurance – minimum level of cover £5,000,000* *Professional Indemnity – minimum level of cover £2,000,000*

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.

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 REDACTED

22. Key Sub-Contractors REDACTED

23. Contract Charges
REDACTED

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:	X Select date	X Select Data

PART B – THE SCHEDULES

Remove all guidance when complete

SCHEDULE 1 – SERVICES NEEDED

The purpose of this Contract is to aid the Department for Transport understand research into cyber security in the transport sector from around the world and how this might translate into a viable cyber incident. Department for Transport may be referred to as the Authority, hereafter.

The Final Report arising from this Contract will then be used within the Authority to support its knowledge base and inform policy development in this field.

SCHEDULE 2 - HIGH LEVEL DELIVERY PLAN

REDACTED

SCHEDULE 3 - BUYER RESPONSIBILITIES

REDACTED

SCHEDULE 4 – NON-DISCLOSURE AGREEMENT

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:	02/01/2018
SoW Reference:	CCSN17A23
Buyer:	REDACTED
Supplier:	REDACTED
Sub-Contractors: *(list all sub-contractors)*	n/a
Overall Estimated Service Completion Date: *(the "Completion Date")*	28/02/2018
Duration of SoW *(How long the SoW will last – expressed as Working Days)*	8 weeks
Charging Mechanism(s) for this SoW: *(Capped/ Time and Materials/ Time and Materials/ Fixed Price/ Milestone deliverables)*	Capped

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	***REDACTED***	

REDACTED	***REDACTED***	
REDACTED	***REDACTED***	
REDACTED	***REDACTED***	

Deliverables:

- i. A draft report. A draft report shall be provided ahead of the project finish to the Authority. This will allow the Authority to provide feedback for the final report. The final report shall be accompanied by an oral presentation of the key findings of the review. Due at the end of week six of the contract period

- ii. A Final report: The Supplier shall deliver a report detailing cyber security research that has been undertaken in the past 5 years that is relevant to the transport modes detailed in section 5.3. below. The report will also detail cyber incidents from around the world from the past 5 years that have a relevance to transport. Due at the end of the project (week 8).

1. PURPOSE

1.1. The purpose of this study is to aid the Department for Transport understand research into cyber security in the transport sector from around the world and how this might translate into a viable cyber incident. Department for Transport may be referred to as the Authority, hereafter.

1.2. The report will then be used within the Authority to support its knowledge base and inform policy development in this field.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1. The Department for Transport (DfT) is the lead Government Department for cyber security in the transport domain.

2.2. The Authority also works with agencies and partners to support the transport network that helps the UK's businesses and gets people and goods travelling around the country. The Authority plans and invests in transport infrastructure to keep the UK on the move.

2.3. The priorities are:

2.3.1. Boosting economic growth and opportunity
2.3.2. Building a One Nation Britain
2.3.3. Improving journeys
2.3.4. Safe, secure and sustainable transport

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1. With incidents growing in prominence and hitting the headlines more frequently cyber security is becoming increasingly essential for many sectors to ensure that are properly protected, this includes the transport sector.

3.2. As the Authority is the lead for the cyber security of the transport sector there is a need to ensure it is up to date on the latest research and incidents.

4. DEFINITIONS

Expression or Acronym	Definition
DfT	Department for Transport
AODB	airport operating databases
SCADA	Supervisory control and data acquisition

5. SCOPE OF REQUIREMENT

5.1. The first stage of the project should review cyber security research from the past 5 years that may be relevant to the aviation, maritime, rail or automotive sectors.

5.2. The second stage of the project should review cyber incidents from around the world covering the last 5 years and identify any which have affected the transport modes listed in section 5.3, and then if possible offer a trend analysis of these incidents.

5.3. The scope for this research does not include company's or operator's back end systems or corporate IT, unless specifically stated below. The scope, per transport mode, does include:

5.3.1. Aviation: aircraft-based systems, air traffic management and control systems, airport systems including airport operating databases (AODB), gate-link systems, access control systems, check in systems, ticket booking systems, operational technology and engineering systems, security screening systems and equipment, baggage and cargo handling systems, passenger information screens and systems.

5.3.2. Maritime: vessel-based systems, vessel traffic management systems, port systems including port community systems, cargo and terminal management systems, access control systems, passenger and cargo check-in systems, operational technology and engineering systems, passenger information screens and systems.

5.3.3. Rail: Suggest rolling stock (passenger and freight), signalling systems, station information displays, ticket barriers, CCTV systems and Traffic Management Systems and SCADA systems.

5.3.4. Roads: road vehicles, connected infrastructure including road signals, traffic lights, and signage.

5.4. The reporting of incidents should be drawn from around the world and can include official cyber security firm reports, news reports, academic publications, and where appropriate blog or other reports. It would be expected that the relevance and authenticity would be assessed by the supplier before any reports are included in the final report.

5.5. The work will not aim to produce a government policy paper but to provide a report which could be used in the formation of such a paper and a database wherein the results may be readily searched.

6. THE REQUIREMENT

6.1. The Supplier shall deliver a report detailing cyber security research that has been undertaken in the past 5 years that is relevant to the transport modes detailed in section 5.3. The report will also detail cyber incidents from around the world from the past 5 years that have a relevance to transport. Within this the Supplier shall:

6.1.1. Detail research that has been found and break it down by transport mode, detailing any overlaps or links between modes.

6.1.2. Give an appraisal of the research that has been found as well as those who undertook it and its source, for example; university researchers, cyber security firms and security researchers.

6.1.3. Identify cyber incidents from around the world from the past five years that have had an effect on transport or may be relevant.

6.1.4. If applicable offer a trend analysis of the incidents identified, for example if one type of attack has grown or been seen regularly, or if one transport mode has been targeted more than others.

6.2. For each item of research or incident identified the report should identify:

6.2.1. the transport asset affected

6.2.2. the attack surface or vulnerabilities identified

6.2.3. what type of attack may be conducted

6.2.4. any reported consequence that may arise from a successful attack, including likely extent of any incident

6.2.5. the type of article (e.g. research, reported vulnerability, or incident)

6.2.6. the year of the article

6.2.7. the organisation behind the research/article or suspected of perpetrating the incident

6.2.8. a link to any originating reference material

6.3. The report should include summaries of both the research findings and the incident findings.

6.4. The project should also provide a readily searchable database of the incidents and research found that can be used to identify or interrogate the information found. This may be in a Microsoft product or a format that is agreed between the parties that can be run on Authority systems. This could be a spreadsheet or pdf or other software we have. This should be covered by the above statement that it will be agreed between the parties.

6.5. A draft report shall be provided ahead of the project finish to the Authority. This will allow the Authority to provide feedback for the final report. The final report shall be accompanied

by an oral presentation of the key findings of the review. This shall be conducted at Authority premises.

7. KEY MILESTONES

7.1. The Supplier should note the following project milestones that the Authority will measure the quality of delivery against:

Milestone	Description	Timeframe
1	An Inception meeting to clarify project deliverables and plan, above that provided in bid documentation.	Will complete within the first week of launch of event.
2	Fortnightly progress reports. (See 16.1)	Fortnightly, following commencement of contract.
3	Draft report covering progress to date	Will complete by week 6 of contract
4	Final report delivery and presentation	Will complete by the final week (week 8) of the contract

7.2. The Supplier shall perform its obligations so as to achieve each Milestone by the Milestone Date.

7.3. Changes to the Milestones shall only be made in accordance with the variation procedure and provided that the Supplier shall not attempt to postpone any of the Milestones using the variation procedure or otherwise (except in the event of an Authority default which affects the Supplier's ability to achieve a Milestone by the relevant Milestone Date).

8. AUTHORITY'S RESPONSIBILITIES

8.1. The Authority will need to ensure that sign-off and comments on the final report is provided as per the agreed timetable.

9. REPORTING

9.1. Please refer to the Suppliers' key reporting responsibilities as mentioned in 7.1. And 16.1.

10. VOLUMES

10.1. One draft report due at the end of week six of the contract period. A final report for delivery and presentation due at the end of the project (week 8).

11. CONTINOUS IMPROVEMENT

11.1. The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

11.2. The Supplier should present new ways of working to the Authority during any Contract review meetings at the beginning and end of the contract, as well as during regular telephone catch ups.
11.3. 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.

12. SUSTAINABILITY

12.1. N/A

13. QUALITY

13.1. The Supplier shall ensure they provide a product that is of a high quality and meets the needs of the requirements as described by the Authority in section six (6), both in terms of the information it provides and in the manner that the information is provided.

14. PRICE

14.1. The Supplier shall provide a capped cost price for this work. Payment is made at the end of the project following satisfactory delivery of all deliverables and acceptance of them by the Authority.

14.2. Prices are to be submitted via the e-Sourcing Suite, Appendix E excluding VAT. Prices should not appear anywhere else in the bid documentation.

15. STAFF AND CUSTOMER SERVICE

15.1. The Authority requires the Supplier to provide a sufficient level of resource throughout the duration of Contract in order to consistently deliver a quality service to all Parties.

15.2. Supplier's staff assigned to Contract shall demonstrate relevant qualifications and experience in the field and how they will use this to deliver the Contract.

15.3. 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.

16. SERVICE LEVELS AND PERFORMANCE

16.1. The Authority will measure the quality of the Supplier's delivery through assessment of their progress alongside the agreed milestones set out in paragraph 7.1:

KPI/SLA	Service Area	KPI/SLA description	Target
#1	Progress Report	Progress reports will be supplied to the DfT project manager by phone or email (to be confirmed). This will include a summary of progress against the delivery.	Fortnightly
#2	Risk monitoring	The Supplier will raise any concerns about the possibility of failing to meet the overall deadline and lack of relevant information to meet the	Within 24 hours

		requirements. Key risks to be monitored should be identified and tracked to ensure the project delivers.	
#3	Communication	The Supplier shall acknowledge any communications from the contract/project manager within 48 working hours.	Within 48 hours
#4	Emergencies	If there is an urgent issue, the Supplier shall make the contact with the project manager within 48 working hours.	Within 48 hours

17. SECURITY REQUIREMENTS

17.1. The Supplier must be able to handle and store classified material up to OFFICIAL level. The project report will be classified at OFFICIAL.

17.2. The Supplier will adhere to the following measures to keep this information secure.

17.3. The Supplier must ensure the security of the information in transit.

17.4. Any electronic files should be stored on an IT system that has access controls that only allow approved personnel with a genuine 'need to know' to access them to read and copy. The IT system should be protected by an appropriate firewall.

17.5. Once electronic files are no longer needed they should be deleted from the IT system in a way that makes recovery unlikely, either by overwriting the storage space or eventual dilution and deterioration on a busy shared storage system.

17.6. Any electronic files or data should be stored within the UK.

17.7. Paper copies (including drafts and notes) and any removable electronic storage must be locked away when not in use to prevent unauthorised access. Printed material should be marked OFFICIAL.

17.8. Paper and printed material should be shredded when no longer needed.

17.9. Access to all material generated by this project (not included source data unless supplied by DfT) must be on a limited and controlled basis, by persons notified to and approved by the DfT.

17.10. The Supplier should have or be seeking to have Cyber Essentials certification.

17.11. Any personal information obtained under this contract must be controlled in compliance with the Data Protection Act.

17.12. Further information on security classification is available on the Cabinet Office website at the following addresses:

REDACTED

18. PAYMENT

18.1. Prices should be submitted in pounds sterling and be inclusive of expenses and exclusive of VAT.

18.2. Invoice to be submitted to the Authority on completion of the contract and acceptance of all deliverables by the Authority.

18.3. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

18.4. Invoices MUST state a relevant Purchase Order Number and be sent to:

REDACTED
REDACTED
REDACTED
REDACTED

18.5. The Authority shall pay the Supplier within Thirty (30) calendar days of receipt of a valid invoice, paid against a valid Purchase Order issued by the Authority; the method of payment will be by BACS.

19. ADDITIONAL INFORMATION

19.1. The Supplier shall agree not to publicise their involvement in this work without the express authorisation of the Authority.

20. LOCATION

20.1. The location of the Services will be carried out at the Supplier's premises. The base location will be the Authority's London office based at:

REDACTED
REDACTED
REDACTED
REDACTED
REDACTED

20.2. The Supplier shall travel to the Authority's premises for a maximum of 3 meetings. Travel to any other locations will only be permitted with prior permission of the Authority and will be at the Authority's T&S rates.

Contract Charges:

The Maximum Price for this SoW is: £73,405.98. This Price is comprised as follows:

Staff member name	Basic Tasks Assigned	Daily Rate	Max. no. of days' input	Total
STAFF GRADE A				
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
STAFF GRADE B				
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
STAFF GRADE C				
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
		Totals:	REDACTED	**£73,405.98**

The Supplier will submit one invoice for £73,405.98 on provision of all Contracted Deliverables to the Authority. The Authority will pay correct and valid invoices within 30 days of receipt.

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