Crown Commercial Service

G-Cloud 12 Call-Off Contract

701570389
The Provision of a Defensive Information Warfare Platform (DInfoCom/0188)

Dated: 06 Aug 2021

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

Part A: Order Form 1
- Call-Off Schedule 1a: Services (Statement of Requirement) 9
- Call-Off Schedule 1b: Services (Suppliers Response) 10
- Call-Off Schedule 2: Call-Off Contract Charges 18

Part B: Terms and Conditions 21
- Call-Off Schedule 3: Collaboration agreement (Not Applicable) 38
- Call-Off Schedule 4: Alternative clauses (Not Applicable) 38
- Call-Off Schedule 5: Guarantee (Not Applicable) 38
- Call-Off Schedule 6: Glossary and Interpretations 39
- Call-Off Schedule 7: GDPR Information 49
- Call-Off Schedule 8: Exit Plan 51
- Call-Off Schedule 9: Statement Relating to Good Standing 52
- Call-Off Schedule 10: Cyber Implementation Plan 55
- Call-Off Schedule 11: Monthly Statement of Work Template 56
- Call-Off Schedule 12: Tasking Order Process Map & Form 57
- Call-Off Schedule 13: Expenses Policy 61

Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	6945 1678 5778 189
Call-Off Contract reference	701570389 (DInfoCom/0188)
Call-Off Contract title	The Provision of a Defensive Information Warfare Platform
Call-Off Contract description	Provide online cloud-based services in order to mentor and up-skill personnel and enable a DIW capability by the Initial Operating Capability (IOC) date of 31 Mar 22. 6 (UK) Div also require the commensurate contractor's technical cloud-based infrastructure to conduct DIW activities. Part of the requirement from the industry partner is to train 6 (UK) Div DIW operators up to the requite standard to safely build their own infrastructure in the future. This is split into 5 separate requirements running concurrently.
Start Date	06 Sep 2021
Expiry Date	05 Sep 2022 The Authority has the Option to exercise 2 x 12 Month Option Periods.
Call-Off Contract value	Year 1 - £936,985.46 (ex VAT). Non-Guaranteed Ad-Hoc Tasking Value (AHTV): £5,000,000.00 ex VAT. Option Year 2 - £307,124.40 (ex VAT) Option Year 3 - £ £307,124.40 (ex VAT) (Option Years Currently unfunded)
Charging method	Capped Time and Materials via CP&F
Purchase order number	TBC

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form.

From the Buyer	Toni Prince MCIPS 030 0164 8453 D Info Commercial, Army HQ, Blenheim Bldg Monxton Road Andover Hampshire SP11 6HJ
To the Supplier	Accenture (UK) Limited +44 (0)20 7844 4000 1 Plantation Place, 30 Fenchurch Street, London EC3M 3BD, United Kingdom Company number: 4757301
Together the 'Parties'	

Principal Contact Details

For the Buyer:

Title:	D Info Commercial SO2
Name:	Sophie Davis
Email:	Sophie.Davis327@mod.gov.uk
Phone:	[REDACTED]

For the Supplier:

Title:	Managing Director
Name:	Madeline Lewis
Email:	madeline.h.lewis@accenture.com
Phone:	[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **06 September 2021** and is valid for twelve (12) months. The date and number of days or months is subject to clause 1.2 in Part B below.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for **two (2)** period(s) of **up to twelve (12) months** each, by giving the Supplier **three (3) months** written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer Contractual Details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot	This Call-Off Contract is for the provision of Services under: Lot 3: Cloud support
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: • Scope and deliver Cyber technical training plan(s) • Provide technical training and verification of that training through exercise(s). • Provide oversight/governance training and verification of that training through exercise(s) • Assist with deployment processes and governance • Plan and deliver an infrastructure (suggestion is Cloud based) that the chosen supplier maintains throughout the contract, including assistance with its accreditation. • Provide ongoing cloud support, mentoring and an “advice service” throughout the contract period for a minimum force of 12 personnel
Additional Services	Not Applicable.
Location	The Services will be delivered to South-West England and Wales as per the Statement of Requirement. **Note**. The exact locations will be made available to the successful Supplier upon Contract Award.

Quality standards	The quality standards required for this Call-Off Contract are as detailed in Schedule 1a – Services: Statement of Requirement.
Technical standards:	The technical standards used as a requirement for this Call-Off Contract as detailed in Schedule 1a Services: Statement of Requirement.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as detailed in Schedule 1a Services: Statement of Requirement.
Onboarding	The onboarding plan for this Call-Off Contract is detailed with Schedule 1b – Services: Supplier Response.
Offboarding	The offboarding plan for this Call-Off Contract is within the Exit Plan detailed at Schedule 8.
Collaboration agreement	Not Applicable.
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed **£1,000,000.00 ex VAT.** The annual total liability for Buyer Data Defaults will not **£1,000,000.00 ex VAT** or **125%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other Defaults will not exceed the greater of **£1,000,000.00 ex VAT** or **125%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Insurance	The insurance(s) required will be: • a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract subject to the Supplier arranging the cover requirements set out below on an annual basis with an insurer of good standing; • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law); and • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than **30** consecutive days.
Audit	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: Clause 7.6 & 7.7 of the Framework Agreement
Buyer's responsibilities	The Buyer is responsible for the provision of Security Passes onto Site and other Sites as directed.
Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes:

	Corporate Laptop and email System (MODNET)

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners: Not Applicable

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is through Contracting, Purchasing & Finance (CP&F) (Exostar).
Payment profile	The payment profile for this Call-Off Contract is based on the Monthly Statement of Work (see Call-Off Schedule 11), in accordance with the Resources and Rates detailed in Call-Off Schedule 2.
Invoice details	The Supplier will issue electronic invoices **monthly** in **arrears**. The Buyer will pay the Supplier within **30** days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to: 6UKXX-FD-SO3, Stuart.Henderson301@mod.gov.uk and cc: Sophie.Davis327@mod.gov.uk
Invoice information required	All invoices must include: • Contract reference, • PO reference, • Work undertaken, • Number of resources, • Number of days, • Day rate, • UIN against associated requirement.
Invoice frequency	Invoice will be sent to the Buyer **monthly**.
Call-Off Contract value	The breakdown of the Charges is: **Core**: Call-Off Charges for the twelve (12) month Core will be in accordance with the agreed Monthly Statement of Work (Call-Off Schedule 11) and the Firm Price Man Days Rates (Call-Off Schedule 2) to a maximum of £936,985.46 ex VAT. (T&S not applicable to Core). **Options**: Call -Off charges for the Option Periods will be in accordance with the agreed Monthly Statement of Work (Call-Off Schedule 11) and the Firm Price Man Days Rates (Call-Off Schedule 2) to a maximum of:

	• Option Year 1 - £307,124.40 (ex VAT) Currently Unfunded, • Option Year 2 - £307,124.40 (ex VAT) Currently Unfunded, (AUTHORITY TO EXERCISE OPTION IF REQUIRED THREE (3) MONTHS PRIOR TO EXPIRY OF CONTRACT). **Non-Guaranteed Ad-Hoc Tasking Value (AHTV):** The Ad-Hoc Tasking Order Form (Call-Off Schedule 12) will be agreed between the Supplier and the Authority, for additional outcomes as and when required, at a maximum cost utilising the Firm Priced Man Day Rates (Call-Off Schedule 2). Ad-Hoc Task costs will fall out of the Non-Guaranteed AHTV of £5,000,000.00 ex VAT. (T&S will be in accordance with Call-Off Schedule 13: Expenses Policy).
Call-Off Contract charges	The breakdown of the Charges is detailed within Schedule 2.

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones: As detailed within the Supplier Response – Schedule 1b and the Exit Plan at Schedule 8.
Guarantee	Not Applicable.
Warranties, representations	Not Applicable.
Supplemental requirements in addition to the Call-Off terms	Not Applicable.
Alternative clauses	Not Applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms	Within the scope of the Call-Off Contract, the Supplier will adhere to the following Defence Conditions: DEFCON 5J (Edn 18/11/16) Unique Identifiers DEFCON 76 (Edn 06/21) Contractors Personnel at Government Establish-ments DEFCON 90 (Edn 06/21) Copyright DEFCON 91 (Edn 06/21) Intellectual Property Rights in Software DEFCON 129J (Edn 18/11/16) The Use of Electronic business Delivery Form DEFCON 513 (Edn 11/16) Value Added Tax DEFCON 514 (Edn 08/15) Material Breach DEFCON 515 (Edn 06/21) Bankruptcy and Insolvency DEFCON 516 (Edn 04/12) Equality DEFCON 518 (Edn 02/17) Transfer DEFCON 520 (Edn 05/18) Corrupt Gifts and Payments of Commission DEFCON 522 (Edn 11/117) Payment and Recovery of Sums Due DEFCON 526 (Edn 08/02) Notices

	DEFCON 527 (Edn 09/97) Waiver DEFCON 529 (Edn 09/97) Law (English) DEFCON 531 (Edn 11/14) Disclosure of Information DEFCON 532B (Edn 04/20) Protection of Personal Data (Where Personal Data is being processed on behalf of the Authority) DEFCON 534 (Edn 06/21) Subcontracting and Prompt Payment DEFCON 537 (Edn 06/02) Rights of Third Parties DEFCON 539 (Edn 08/13) Transparency DEFCON 550 (Edn 02/14) Child Labour/Employment Law DEFCON 566 (Edn 10/20) Change of control of contractor DEFCON 602B (Edn 12/06) Quality Assurance (without Quality Plan) DEFCON 604 (Edn 06/14) Progress Reports DEFCON 611 (Edn 02/16) Issued Property DEFCON 625 (Edn 06/21) Co-operation on Expiry of Contract DEFCON 632 (Edn 06/21) Third Party Intellectual Property – Rights and Restrictions DEFCON 642 (Edn 06/14) Progress Meetings DEFCON 658 (Edn 10/17) Cyber Note: Further to DEFCON 658 the Cyber Risk Profile of the Contract is High as defined in DEF-STAN 05-138. DEFCON 659A (Edn 06/21) Security Measures DEFCON 660 (Edn 12/15) Official-Sensitive Security Requirements DEFCON 694 (Edn 07/18) Accounting for Property of the Authority **AUTHORISATION BY THE CROWN FOR USE OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS** Notwithstanding any other provisions of the Contract and for the avoidance of doubt, award of the Contract by the Authority and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Contractor acknowledges that any such authorisation by the Authority under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.
Public Services Network (PSN)	Not Applicable.
Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1.

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.

2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	Supplier	Buyer
Name	Brendan Wilkins	Toni Prince MCIPS
Title	Managing Director	Army D Info Commercial SCO
Signature	[REDACTED]	[REDACTED]
Date	20/08/2021	24/08/2021

Call-Off Schedule 1a: Services (Statement of Requirement)

701570389

THE PROVISION OF A DEFENSIVE INFORMATION WARFARE PLATFORM

(DInfoCom/0188)

STATEMENT OF REQUIREMENT

CONTENTS

1. BACKGROUND 2
2. DURATION 2
3. SCOPE OF REQUIREMENT 2
4. REQUIREMENT 1 2
5. REQUIREMENT 2 4
6. REQUIREMENT 3 5
7. REQUIREMENT 4 6
8. REQUIREMENT 5 7
9. PROGRESS MEETINGS 7
10. SECURITY REQUIREMENTS 7
11. INTELLECTUAL PROPERTY RIGHTS (IPR) 7
12. EXIT PLAN 7
13. IR35 8
14. TRAVEL AND SUBSISTENCE 8
15. CONTINUOUS IMPROVEMENT 8

1. BACKGROUND

1.1 The MoD may be referred to as "the Authority" hereafter.

1.2 6 (UK) Div is mandated to provide unconventional warfare capabilities, delivered through its Units.

1.3 It is desirable for an NCSC approved Supplier to provide a cloud hosted Cyber Training Environment with the ability to test and train White Team's, Red Team's and Blue Teams. Support, mentoring, and training are required to use this cloud hosted training system, the longer-term requirement will be met by MoD sponsored programmes.

1.4 This Statement of Requirement (SOR) supports the intermediate requirement for training, cloud hosting and supporting services to deliver these capabilities. While related courses are available across Defence, there are no systems which can currently meet the specific operational training requirements of the capabilities.

2. DURATION

2.1 The duration of the requirement is for a twelve (12) month period, from 06 Sep 2021 until 05 Sep 2022, with 2 x twelve (12) month option periods.

3. SCOPE OF REQUIREMENT

3.1 DIW requires a blend of skills in order to acquire the requisite information and data to conduct Information Activities. 6 (UK) Div currently lack sufficient cyber technical knowledge, skills, and experience to test and develop a Defensive Information Warfare (DIW) Platform independently. 6 (UK) Div therefore requires a trusted industry partner to provide online cloud-based services in order to mentor and up-skill personnel and enable a DIW capability by the Initial Operating Capability (IOC) date of 31 Mar 22.

3.2 6 (UK) Div also require the commensurate contractor's technical cloud-based infrastructure to conduct DIW activities. Part of the requirement from the industry partner is to train 6 (UK) Div DIW operators up to the requite standard to safely build their own infrastructure in the future. This is split into 5 separate requirements running concurrently.

4. REQUIREMENT 1

4.1 **Location**: South-West England.

Ser	Equipment/Services	Duration	Comment
1	a. Conduct initial base line meetings / scoping study to determine level of support. b. Initial meeting to define hosting requirements, feasibility of proposed activities.	2 weeks	Initial support to define cloud hosting infrastructure requirements, training requirements and feasibility of proposed activities.
2	Deliver Cyber technical training plan including Confirmatory and final exercise deliverables and standards.	2 weeks	Provision of technical pen testing training solution for 12 soldiers to include: a. Provision and maintenance of infrastructure, b. Assess vulnerabilities in ITC systems. *(to be delivered after Ser 1)*

3	Advise and facilitate provision of hosting environment.	2 weeks	A detailed plan outlining the agreed deliverables will be agreed during the initial meeting. *(to be delivered after Ser 1)*
4	a. Deliver training, as agreed at serial 2 and suitable training environment for a minimum of 12 soldiers. b. Provision and testing of online engagement infrastructure. c. Assessing vulnerabilities in and protecting own infrastructure. d. Training of 12 DIW operators to an entry level standard (to be agreed in the training plan). e. Initial infrastructure to enable DIW operational training. f. Planning build up and delivery of a Final Test Exercise (FTX).	*14 weeks* *(Not including Christmas stand-down 20 Dec 2021 - 02 Jan 2022)*	The timeline from on contract until IOC will be 18 weeks (*Not including Christmas stand-down 20 Dec 2021 - 02 Jan 2022)* to include: a. Initial scoping study – 2 weeks. b. Build – 2 weeks. c. Pre-training by contractor – 2 weeks *(may be concurrent with a. and b.)* d. Pen test bootcamp to include 2-day confirmation exercise. – 6 weeks. e. Final Test Exercise (FTX). 5 days set up and build/ 5 days FTX. *(Standards to be agreed in serial 2).*
5	A post project report, documenting deliverables, training plan, methodology and cost, outlining lessons learned and recommendations.	2 weeks	*(delivered after ser 4)*
6	a. Provide an ongoing cloud support, mentoring and advice service throughout the contract period for a minimum of 12 personnel. b. Provide a continuous use representative training environment to practice procedures including representative exercises for a minimum of 12 personnel.	Initial 1 year	For the duration of the contract.
7	In consultation with the Authority ensure all systems are accredited for use and compliant with UK law and Defence policies.	Initial 1 year	For the duration of the contract.

5. REQUIREMENT 2

5.1 **Location**: Wales or South-West England.

Ser	Equipment/Services	Duration	Comment
1	a. Conduct initial base line meetings / scoping study to determine level of support. b. Initial meeting to define hosting requirements, feasibility of proposed activities.	2 weeks	Initial support to define cloud hosting infrastructure requirements, training requirements and feasibility of proposed activities.
2	Deliver Cyber technical training plan including Confirmatory and final exercise deliverables and standards.	2 weeks	Provision of technical pen testing training solution for 12 soldiers to include: a. Provision and maintenance of infrastructure. b. Assess vulnerabilities in ITC systems. c. Training for the operation and configuration of SDR (Software Defined Radio) based equipment. *(delivered after Ser 1)*
3	Advise and facilitate provision of hosting environment.	2 weeks	A detailed plan outlining the agreed deliverables will be agreed during the initial meeting. *(delivered after Ser 1)*
4	a. Deliver training, as agreed at serial 2 and suitable training environment for a minimum of 12 soldiers. b. Provision and testing of online engagement infrastructure. c. Assessing vulnerabilities in and protecting own infrastructure. d. Training of 12 DIW operators to an entry level standard (to be agreed in the training plan). e. Initial infrastructure to enable DIW operational training. f. Planning build up and delivery of a Final Test Exercise (FTX).	14 weeks *(Not including Christmas stand-down 20 Dec 2021 - 02 Jan 2022)*	The timeline from on contract until IOC will be 18 weeks *(Not including Christmas stand-down 20 Dec 2021 - 02 Jan 2022)* to include: a. Initial scoping study – 2 weeks. b. Build – 2 weeks. c. Pre-training by contractor – 2 weeks (may be concurrent with a. and b.) d. Pen test bootcamp to include 2-day confirmation exercise. – 6 weeks. e. Final Test Exercise (FTX). 5 days set up and build/ 5 days FTX. *(Standards to be agreed in serial 2.)*

5	A post project report, documenting deliverables, training plan, methodology and cost, outlining lessons learned and recommendations.	2 weeks	*(delivered after ser 4)*
6	a. Provide an ongoing cloud support, mentoring and advice service throughout the contract period for a minimum of 12 personnel. b. Provide a continuous use representative training environment to practice procedures including representative exercises for a minimum of 12 personnel.	Initial 1 year	For the duration of the contract.
7	In consultation with the Authority ensure all systems are accredited for use and compliant with UK law and Defence policies.	Initial 1 year	For the duration of the contract.

6. REQUIREMENT 3

6.1 **Location**: South-West England.

Ser	Equipment/Services	Duration	Comment
1	Conduct initial base line meetings / scoping study to determine requirements and level of support.	2 weeks	Initial support to define requirements and feasibility of proposed activities.
2	Conduct development of info graphic's with supporting documentation for the scope and deployment constraints/freedoms of Defence Info Activities (DIA) and cyber capabilities within Requirements 1 and 2. This should be in terms of effects generated but with clear linkages to technologies/skillsets used in delivery.	2 weeks	Provision of technical training solution for 12 soldiers to include: a. Provision and maintenance of infrastructure. b. Assess vulnerabilities in ITC systems. *(delivered after Ser 1)*
3	Development of XDLOD capability roadmap linked to deliverable above to develop task line for operational use. This should identify quick wins with longer term, bigger	2 weeks	*(delivered after Ser 1)*

	impact. capabilities having assessed current capability baseline.		
4	Development of deployment procedures (within current the authorisations and policies) for capabilities prioritised in the capability roadmap (build the White Team).	2 weeks	*(delivered after Ser 1)*
5	Deliver White team training and suitable training environment for 30 soldiers to enable a final test exercise to demonstrate White Team competencies.	10 days – 3 weeks	Enable a final test ex to demonstrate White Team competencies. *(delivered after Ser 2,3 and 4)*
6	Test exercise based on real world scenarios for a White Team lead operation.	2 weeks	*(delivered after ser 5)*
7	A post training report outlining lessons learned and recommendations.	2 weeks	*(delivered after ser 6)*
8	Support for a deployment for Unit to Red Team against blue forces on operations	6 weeks	*(delivered after ser 7)*
9	Provide an ongoing cloud support, mentoring and advice service throughout the contract period.	Initial 1 year	For the duration of the contract.
10	In consultation with the Authority ensure all systems are accredited for use and compliant with UK law and Defence policies.	Initial 1 year	For the duration of the contract.

7. REQUIREMENT 4

Ser	Equipment/Services	Duration	Comment
1	a. Ability to call off further cloud hosted environments, training, support and mentoring as training plans develop. b. Ability to call off Operational concept demonstrate and exercises to demonstrate Organisational competence.	As required.	Follow on requirements to be requested via an Ad-Hoc Tasking Order Form.

8. REQUIREMENT 5

Ser	Equipment/Services	Duration	Comment
1	a. Completion of all Risk Management documentation to cover the full contract including DPIA compliance working with the Army/MOD for approval. b. Quarterly Security working group including contract start meeting to document and agree accreditation and DPIA roles and responsibilities.	Initial 1 year.	a. Supplier to ensure the intended use can occur within extant MOD Legal policy permissions /exemptions, which may apply even if developed by a contractor working with Army/MOD. b. Supplier to be responsible for DPA 18 and DPIA compliance risks subject to the Authority following suppliers' instructions.

9. PROGRESS MEETINGS

9.1 Quarterly stakeholder and commercial review meeting including contract start meeting.

9.2 Fortnightly project meeting.

9.3 Stakeholder brief after completion of Requirements 1, 2 and 3.

9.4 Quarterly Security working group including contract start meeting.

9.5 No other communications or engagement should be carried out on this project without written approval of SO1 FD, 6 (UK) Div.

10. SECURITY REQUIREMENTS

10.1 The delivery partner must:

10.1.1 Hold UK GOV DV security clearance.

10.1.2 Hold industry recognised expertise such as the Council for Registered Ethical Security Testers (CREST) accreditation.

10.1.3 Have recent experience with the last three years with UK GOV cyber operations and training provision.

10.2 It is desirable that the delivery partner is NCSC assured.

11. INTELLECTUAL PROPERTY RIGHTS (IPR)

11.1 All IP generated during the contract remains the property of the Authority. The Supplier shall not retain IPR relating to any services delivered during the terms of the contract.

12. EXIT PLAN

12.1 The Authority and the Supplier will agree an exit plan during the Call-Off Contract period to enable the Supplier Deliverables to be transferred to the Authority ensuring that the Authority has all the documentation required to support and continuously develop the Service with Authority resource or any third party as the Authority requires. The Supplier will update this plan whenever there are material changes to the Services. A Statement of Work (SoW) may be agreed between the Authority and the Supplier to specifically cover the exit plan.

13. IR35

13.1 The MOD is required to inform the Supplier whether the off-payroll rules apply or not, and in so doing is also required to provide the reasons for reaching the outcome.

13.2 We have assessed that under the Intermediaries legislation, the Off-payroll working rules do not apply to this engagement.

13.3 This decision has been derived by assessing the requirement in full utilising the following criteria:

Consideration		Indicators of a supply of a managed service
1	How are the deliverables articulated?	Deliverables will be outcome based with the detail of the outcomes clearly specified in the contract with the Supplier.
2	Who do you articulate the deliverable to?	Deliverables will be articulated to the Supplier. The Supplier will tell the worker(s) what is required of them to deliver the contract.
3	Is the worker under the day to day direction or control of MOD or Supplier?	The worker will be under the day to day direction and control of the Supplier.
4	Who does MOD go to if there is an issue with the quality of service?	MOD will raise quality or non-delivery issues with the Supplier not the resource.
5	Where does the risk of failure sit?	The Supplier will be held accountable for non-delivery of the requirements specified in the contract.
6	Are you looking to hire a specific worker?	MOD will not care who the Supplier sends to perform the work / deliver the service as long as the appropriate SQEP resource is provided.

14. TRAVEL AND SUBSISTENCE

14.1 Travel and Subsistence (T&S) must be in line with the MOD expenses policy. (see Call-Off Schedule 13: Expenses Policy).

15. CONTINUOUS IMPROVEMENT

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

15.2 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.

Call-Off Schedule 1b: Services (Suppliers Response)

[REDACTED]

Call-Off Schedule 2: Call-Off Contract Charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

PRICING SCHEDULE FOR: 701570389 (DInfoCom/0188) - The Provision of a Defensive Information Warfare Platform				
Supplier Name:	Accenture (UK) Limited			
PLEASE NOTE:				
CHARGING METHOD: Capped Time and Materials (CTM)				
The total value of the twelve (12) month contract plus 2 x 12-month option periods is what will be evaluated. Any prices not included within Schedule will be deemed to have been waived.				
The Authority will reserve the right to request additional resources, within the scope of the contract, using Tasking Order Forms for shorter term tasks based on the Firm Man Day Rates.				

Table 1: Twelve (12) Month Contract, 06 Sep 2021 - 05 Sep 2022 (Goods & Support)				
Services	SFIA Level	Duration	Cost (£) (Ex VAT) EACH	Total cost (Ex VAT) NOT TO EXCEED
Managing Director	SFIA level 7		[REDACTED]	[REDACTED]
Senior Technical Manager	SFIA level 6		[REDACTED]	
Senior Technical Manager	SFIA Level 5		[REDACTED]	
Technical Manager	SFIA Level 4		[REDACTED]	
Senior Programme Manager	SFIA Level 5		[REDACTED]	
Project Manager	SFIA Level 4		[REDACTED]	
			Sub Total	[REDACTED]

Goods	Product Number	Quantity	Cost (£) (Ex VAT) EACH	Total cost (Ex VAT) NOT TO EXCEED
Requirement 1 (South West England)				
NETGATE 1100 PFSENSE+ SECURITY GATEWAY		2.00	[REDACTED]	[REDACTED]
ProSAFE 8-Port Gigabit Unmanaged Plus Switch (With VLANs, QoS & IGMP Snooping)		1.00	[REDACTED]	[REDACTED]
ProSAFE Jr 24-Port Gigabit Unmanaged Plus Switch (With VLANs, QoS & IGMP Snooping)		1.00	[REDACTED]	[REDACTED]
Dell PowerEdge R640 3 Years Next Business Day Support		1.00	[REDACTED]	[REDACTED]
Latitude 5520 Laptop with 3 Year Pro Support		15.00	[REDACTED]	[REDACTED]
VMware vSphere 7 Essentials Kit for 3 hosts (Max 2 processors per host). Subscription only for VMware vSphere 7 Essentials Kit for 3 years		1.00	[REDACTED]	[REDACTED]
VMware vSphere 7 Essentials Per Incident Support - Email + Phone, 3 incident/year		1.00	[REDACTED]	[REDACTED]
Windows Server 2019 Datacenter Core - 16 Core License Pack		2.00	[REDACTED]	[REDACTED]
Microsoft Office Professional Plus 2019 (KMS)		8.00	[REDACTED]	[REDACTED]
Windows 10 Enterprise LTSC 2019 Upgrade		8.00	[REDACTED]	[REDACTED]
Windows Server 2019 Client Access License - 1 User CAL		8.00	[REDACTED]	[REDACTED]
Exchange Server Standard 2019		1.00	[REDACTED]	[REDACTED]
Exchange Server Standard User CAL 2019		5.00	[REDACTED]	[REDACTED]
Exchange 2019 Outlook License		5.00	[REDACTED]	[REDACTED]
SharePoint Server 2019		1.00	[REDACTED]	[REDACTED]
SharePoint Standard 2019 User CAL		3.00	[REDACTED]	[REDACTED]
SQL Server 2019 Standard Edition		2.00	[REDACTED]	[REDACTED]
Pentesting with Kali - PEN-200 with 60-days lab plus (1) OSCP exam attempt		12.00	[REDACTED]	[REDACTED]
Red Team Ops Course - 60 days lab access		12.00	[REDACTED]	[REDACTED]
			Sub Total	[REDACTED]
Requirement 2 (Wales or South West England)				
NETGATE 1100 PFSENSE+ SECURITY GATEWAY		1.00	[REDACTED]	[REDACTED]
ProSAFE Jr 24-Port Gigabit Unmanaged Plus Switch (With VLANs, QoS & IGMP Snooping)		1.00	[REDACTED]	[REDACTED]
Dell PowerEdge R640 3 Years Next Business Day Support		1.00	[REDACTED]	[REDACTED]
VMware vSphere 7 Essentials Kit for 3 hosts (Max 2 processors per host). Subscription only for VMware vSphere 7 Essentials Kit for 3 years		1.00	[REDACTED]	[REDACTED]
VMware vSphere 7 Essentials Per Incident Support - Email + Phone, 3 incident/year		1.00	[REDACTED]	[REDACTED]
Windows Server 2019 Datacenter Core - 16 Core License Pack		2.00	[REDACTED]	[REDACTED]
Microsoft Office Professional Plus 2019 (KMS)		8.00	[REDACTED]	[REDACTED]
Windows 10 Enterprise LTSC 2019 Upgrade		8.00	[REDACTED]	[REDACTED]
Windows Server 2019 Client Access License - 1 User CAL		8.00	[REDACTED]	[REDACTED]
Exchange Server Standard 2019		1.00	[REDACTED]	[REDACTED]
Exchange Server Standard User CAL 2019		5.00	[REDACTED]	[REDACTED]
Exchange 2019 Outlook License		5.00	[REDACTED]	[REDACTED]
SharePoint Server 2019		1.00	[REDACTED]	[REDACTED]
SharePoint Standard 2019 User CAL		3.00	[REDACTED]	[REDACTED]
SQL Server 2019 Standard Edition		2.00	[REDACTED]	[REDACTED]
			Sub Total	[REDACTED]
Total cost NOT TO EXCEED for the twelve (12) month Contract, 06 Sep 2021 - 05 Sep 2022 (Goods & Support) - Ex VAT				[REDACTED]

Table 2: OPTION PERIOD 1 - Twelve (12) Months, 06 Sep 2022 - 05 Sep 2023 (Goods & Support)				
Services	**SFIA Level**	**Duration**	**Cost (£) (Ex VAT) EACH**	**Total cost (Ex VAT) NOT TO EXCEED**
Managing Director	SFIA level 7		[REDACTED]	[REDACTED]
Senior Technical Manager	SFIA level 6		[REDACTED]	
Senior Technical Manager	SFIA Level 5		[REDACTED]	
Technical Manager	SFIA Level 4		[REDACTED]	
Senior Programme Manager	SFIA Level 5		[REDACTED]	
Project Manager	SFIA Level 4		[REDACTED]	
			Sub Total	[REDACTED]
Goods	**Product Number**	**Quantity**	**Cost (£) (Ex VAT) EACH**	**Total cost (Ex VAT) NOT TO EXCEED**
Requirement 1 (South West England)				
Windows Server 2019 Datacenter Core - 16 Core License Pack		2.00	[REDACTED]	[REDACTED]
Microsoft Office Professional Plus 2019 (KMS)		8.00	[REDACTED]	[REDACTED]
Windows 10 Enterprise LTSC 2019 Upgrade		8.00	[REDACTED]	[REDACTED]
Windows Server 2019 Client Access License - 1 User CAL		8.00	[REDACTED]	[REDACTED]
Exchange Server Standard 2019		1.00	[REDACTED]	[REDACTED]
Exchange Server Standard User CAL 2019		5.00	[REDACTED]	[REDACTED]
Exchange 2019 Outlook License		5.00	[REDACTED]	[REDACTED]
SharePoint Server 2019		1.00	[REDACTED]	[REDACTED]
SharePoint Standard 2019 User CAL		3.00	[REDACTED]	[REDACTED]
SQL Server 2019 Standard Edition		2.00	[REDACTED]	[REDACTED]
Pentesting with Kali - PEN-200 with 60-days lab plus (1) OSCP exam attempt		12.00	[REDACTED]	[REDACTED]
Red Team Ops Course - 60 days lab access		12.00	[REDACTED]	[REDACTED]
			Sub Total	[REDACTED]
Requirement 2 (Wales or South West England)				
Windows Server 2019 Datacenter Core - 16 Core License Pack		2.00	[REDACTED]	[REDACTED]
Microsoft Office Professional Plus 2019 (KMS)		8.00	[REDACTED]	[REDACTED]
Windows 10 Enterprise LTSC 2019 Upgrade		8.00	[REDACTED]	[REDACTED]
Windows Server 2019 Client Access License - 1 User CAL		8.00	[REDACTED]	[REDACTED]
Exchange Server Standard 2019		1.00	[REDACTED]	[REDACTED]
Exchange Server Standard User CAL 2019		5.00	[REDACTED]	[REDACTED]
Exchange 2019 Outlook License		5.00	[REDACTED]	[REDACTED]
SharePoint Server 2019		1.00	[REDACTED]	[REDACTED]
SharePoint Standard 2019 User CAL		3.00	[REDACTED]	[REDACTED]
SQL Server 2019 Standard Edition		2.00	[REDACTED]	[REDACTED]
			Sub Total	[REDACTED]
Total cost NOT TO EXCEED for the twelve (12) month Option Period 1, 06 Sep 2022 - 05 Sep 2023 (Goods & Support) - Ex VAT				[REDACTED]

Table 3: OPTION PERIOD 2 - Twelve (12) Months, 06 Sep 2023 - 05 Sep 2024 (Goods & Support)				
Goods/Service	Product Number	Quantity/ Duration	Cost (£) (Ex VAT) EACH	Total cost (Ex VAT) NOT TO EXCEED
Managing Director	SFIA level 7		[REDACTED]	[REDACTED]
Senior Technical Manager	SFIA level 6		[REDACTED]	
Senior Technical Manager	SFIA Level 5		[REDACTED]	
Technical Manager	SFIA Level 4		[REDACTED]	
Senior Programme Manager	SFIA Level 5		[REDACTED]	
Project Manager	SFIA Level 4		[REDACTED]	
			Sub Total	[REDACTED]
Goods	Product Number	Quantity	Cost (£) (Ex VAT) EACH	Total cost (Ex VAT) NOT TO EXCEED
Requirement 1 (South West England)				
Windows Server 2019 Datacenter Core - 16 Core License Pack		2.00	[REDACTED]	[REDACTED]
Microsoft Office Professional Plus 2019 (KMS)		8.00	[REDACTED]	[REDACTED]
Windows 10 Enterprise LTSC 2019 Upgrade		8.00	[REDACTED]	[REDACTED]
Windows Server 2019 Client Access License - 1 User CAL		8.00	[REDACTED]	[REDACTED]
Exchange Server Standard 2019		1.00	[REDACTED]	[REDACTED]
Exchange Server Standard User CAL 2019		5.00	[REDACTED]	[REDACTED]
Exchange 2019 Outlook License		5.00	[REDACTED]	[REDACTED]
SharePoint Server 2019		1.00	[REDACTED]	[REDACTED]
SharePoint Standard 2019 User CAL		3.00	[REDACTED]	[REDACTED]
SQL Server 2019 Standard Edition		2.00	[REDACTED]	[REDACTED]
Pentesting with Kali - PEN-200 with 60-days lab plus (1) OSCP exam attempt		12.00	[REDACTED]	[REDACTED]
Red Team Ops Course - 60 days lab access		12.00	[REDACTED]	[REDACTED]
			Sub Total	[REDACTED]
Requirement 2 (Wales or South West England)				
Windows Server 2019 Datacenter Core - 16 Core License Pack		2.00	[REDACTED]	[REDACTED]
Microsoft Office Professional Plus 2019 (KMS)		8.00	[REDACTED]	[REDACTED]
Windows 10 Enterprise LTSC 2019 Upgrade		8.00	[REDACTED]	[REDACTED]
Windows Server 2019 Client Access License - 1 User CAL		8.00	[REDACTED]	[REDACTED]
Exchange Server Standard 2019		1.00	[REDACTED]	[REDACTED]
Exchange Server Standard User CAL 2019		5.00	[REDACTED]	[REDACTED]
Exchange 2019 Outlook License		5.00	[REDACTED]	[REDACTED]
SharePoint Server 2019		1.00	[REDACTED]	[REDACTED]
SharePoint Standard 2019 User CAL		3.00	[REDACTED]	[REDACTED]
SQL Server 2019 Standard Edition		2.00	[REDACTED]	[REDACTED]
			Sub Total	[REDACTED]
Total cost NOT TO EXCEED for the twelve (12) month Option Period 2, 06 Sep 2023 - 05 Sep 2024 (Goods & Support) - Ex VAT				[REDACTED]

Part B: Terms and Conditions

1. Call-Off Contract Start Date and Length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of Terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)

- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract';

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer';

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of Services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services;

4.1.2 apply all due skill, care and diligence in faithfully performing those duties;

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer;

4.1.4 respond to any enquiries about the Services as soon as reasonably possible;

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer.

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due Diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000;

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit;

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date;

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date.

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance;

9.4.2 receipts for the insurance premium;

9.4.3 evidence of payment of the latest premiums due.

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers;

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances;

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance.

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly;

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer.

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection

Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.5.1 rights granted to the Buyer under this Call-Off Contract;

11.5.2 Supplier's performance of the Services;

11.5.3 use by the Buyer of the Services.

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.6.1 modify the relevant part of the Services without reducing its functionality or performance;

11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer;

11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer.

11.7 Clause 11.5 will not apply if the IPR Claim is from:

11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.7.3 other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data;

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body;

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes.

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request;

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions;

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer);

12.2.4 providing the Buyer with any information requested by the Data Subject.

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer Data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its

obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.cpni.gov.uk/protection-sensitive-information-and-assets .

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided;

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control.

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided;

18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses.

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied;

18.4.2 any fraud.

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so;

18.5.2 an Insolvency Event of the other Party happens;

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business.

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration;

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry;

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses:

- 7 (Payment, VAT and Call-Off Contract charges),
- 8 (Recovery of sums due and right of set-off),
- 9 (Insurance),
- 10 (Confidentiality),
- 11 (Intellectual property rights),
- 12 (Protection of information),
- 13 (Buyer data),
- 19 (Consequences of suspension, ending and expiry),
- 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability),
- 8.44 to 8.50 (Conflicts of interest and ethical walls),
- 8.89 to 8.90 (Waiver and cumulative remedies).

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it;

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer;

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer;

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law;

19.5.5 work with the Buyer on any ongoing work;

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date.

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer;

21.6.2 there will be no adverse impact on service continuity;

21.6.3 there is no vendor lock-in to the Supplier's Service at exit;

21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice.

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier;

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer;

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier;

21.8.4 the testing and assurance strategy for exported Buyer Data;

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations;

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition.

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control;

22.1.2 other information reasonably requested by the Buyer.

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss

or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form;

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form;

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises;

25.5.2 comply with Buyer requirements for the conduct of personnel;

25.5.3 comply with any health and safety measures implemented by the Buyer;

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury.

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform,

29.2.2 age,

29.2.3 start date,

29.2.4 place of work,

29.2.5 notice period,

29.2.6 redundancy payment entitlement,

29.2.7 salary, benefits and pension entitlements,

29.2.8 employment status,

29.2.9 identity of employer,

29.2.10 working arrangements,

29.2.11 outstanding liabilities,

29.2.12 sickness absence,

29.2.13 copies of all relevant employment contracts and related documents,

29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.6.1 its failure to comply with the provisions of this clause;

29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer.

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors;

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services.

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Call-Off Schedule 3: Collaboration agreement (Not Applicable)

Call-Off Schedule 4: Alternative clauses (Not Applicable)

Call-Off Schedule 5: Guarantee (Not Applicable)

Call-Off Schedule 6: Glossary and Interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner

Data Subject	Takes the meaning given in the GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)

Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium

Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	• induce that person to perform improperly a relevant function or activity
	• reward that person for improper performance of a relevant function or activity
	• commit any offence:
	  ○ under the Bribery Act 2010
	  ○ under legislation creating offences concerning Fraud
	  ○ at common Law concerning Fraud
	  ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.

Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.

Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Call-Off Schedule 7: GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1 to Call-Off Schedule 7: Processing Personal Data

1.1 This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1.1 The contact details of the Buyer's Data Protection Officer are: Maj Steve Gibbs, Steven.Gibbs794@mod.gov.uk.

1.1.2 The contact details of the Supplier's Data Protection Officer are: Tessa O'Brien tessa.obrien@accenture.com.

1.2 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.3 Any such further instructions shall be incorporated into this Annex.

Descriptions	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: The Supplier shall have access to Personal Data as part of the training cycles.
Duration of the Processing	Contract Duration.
Nature and purposes of the Processing	The Supplier may need access to Personal Data in order to support each training cycle.
Type of Personal Data	Name, Student Reference Number
Categories of Data Subject	• Staff • Suppliers

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	The Supplier shall not: • Delete or remove any proprietary notices contained within or relating to the Buyer data; and • Store, copy, disclose or use the Buyer Data except as necessary for the performance by the Supplier of its obligations under this Call off Contract or as otherwise approved by the Supplier At the written request of either Party or at the end each training cycle the Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be appropriate for them to retain such Personal Data under applicable Data Protection Law Legislation and their privacy policy (save to the extent and for the limited period) that such information needs to be retained by the a Party for statutory compliance the purposes of complying with Law or as otherwise required by this Contract), and taking all further actions as may be necessary or desirable to ensure its compliance with Data Protection Law Legislation and its privacy policy.

Annex 2 to Call-Off Schedule 7: Joint Controller Agreement (Not Applicable)

Call-Off Schedule 8: Exit Plan

The Buyer and the Supplier will agree an exit plan during the Call-Off Contract period to enable the Supplier Deliverables to be transferred to the Buyer ensuring that the Buyer has all the code and documentation required to support and continuously develop the Service with Buyer resource or any third party as the Buyer requires. The Supplier will update this plan whenever there are material changes to the Services. A Statement of Work may be agreed between the Buyer and the Supplier to specifically cover the exit plan.

Call-Off Schedule 9: Statement Relating to Good Standing

Statement Relating to Good Standing (PCR 2015)

The Statement Relating To Good Standing

Contract Title: The Provision of a Defensive Information Warfare Platform

Contract Number: 701570389

1. We confirm, to the best of our knowledge and belief, that ***Accenture (UK)*** Limited including its directors or any other person who has powers of representation, decision or control or is a member of the administrative, management or supervisory body of ***Accenture (UK) Limited*** has not been convicted of any of the following offences within the past 5 years:

    a. conspiracy within the meaning of section 1 or 1A of the Criminal Law Act 1977 or article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA;

    b. corruption within the meaning of section 1(2) of the Public Bodies Corrupt Practices Act 1889 or section 1 of the Prevention of Corruption Act 1906;

    c. common law offence of bribery;

    d. bribery within the meaning of section 1,2 or 6 of the Bribery Act 2010; or section 113 of the Representation of the People Act 1983;

    e. any of the following offences, where the offence relates to fraud affecting the European Communities financial interests as defined by Article 1 of the Convention on the protection of the financial interests of the European Communities:

        (1) the common law offence of cheating the Revenue;

        (2) the common law offence of conspiracy to defraud;

        (3) fraud or theft within the meaning of the Theft Act 1968, the Theft Act (Northern Ireland) 1969, the Theft Act 1978 or the Theft (Northern Ireland) Order 1978;

        (4) fraudulent trading within the meaning of section 458 of the Companies Act 1985, Article 451 of the Companies (Northern Ireland) Order 1986 or section 933 of the Companies Act 2006;

        (5) fraudulent evasion within the meaning of section 170 of the Customs and Excise Management Act 1979 or section 72 of the Value Added Tax Act 1994;

        (6) an offence in connection with taxation in the European Union within the meaning of section 71 of the Criminal Justice Act 1993;

        (7) destroying, defacing or concealing of documents or procuring the extension of a valuable security within the meaning of section 20 of the Theft Act 1968 or section 19 of the Theft Act (Northern Ireland) 1969;

        (8) fraud within the meaning of section 2,3 or 4 of the Fraud Act 2006; or

        (9) the possession of articles for use in frauds within the meaning of section 6 of the Fraud Act 2006, or making, adapting, supplying or offering to supply articles for use in frauds within the meaning of section 7 of that Act;

    f. any offence listed:

        (1) in section 41 of the Counter Terrorism Act 2008; or

        (2) in Schedule 2 to that Act where the court has determined that there is a terrorist connection;

g. any offence under sections 44 to 46 of the Serious Crime Act 2007 which relates to an offence covered by (f) above;

h. money laundering within the meaning of section 340(11) and 415 of the Proceeds of Crime Act 2002;

i. an offence in connection with the proceeds of criminal conduct within the meaning of section 93A, 93B, or 93C of the Criminal Justice Act 1988 or article 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996;

j. an offence under section 4 of the Asylum and Immigration (Treatment of Claimants etc) Act 2004;

k. an offence under section 59A of the Sexual Offences Act 2003;

l. an offence under section 71 of the Coroners and Justice Act 2009;

m. an offence in connection with the proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994; or

n. an offence under section 2 or 4 of the Modern Slavery Act 2015;

o. any other offence within the meaning of Article 57(1) of Public Contracts Directive –

(1) as defined by the law of any jurisdiction outside England and Wales and Northern Ireland; or

(2) created in the law of England and Wales or Northern Ireland after the day on which these Regulations were made;

p. any breach of its obligations relating to the payment of taxes or social security contributions where the breach has been established by a judicial or administrative decision having final and binding effect in accordance with the legal provisions of the country in which it is established or with those of any jurisdictions of the United Kingdom.

2. ***Accenture (UK) Limited*** further confirms to the best of our knowledge and belief that within the last 3 years it:

a. has fulfilled its obligations relating to the payment of taxes and social security contributions of the country in which it is established or with those of any jurisdictions of the United Kingdom;

b. is not bankrupt or is not the subject of insolvency or winding-up proceedings, where its assets are being administered by a liquidator or by the court, where it is in an agreement with creditors, where its business activities are suspended or it is in any analogous situation arising from a similar procedure under the laws and regulations of any State;

c. has not committed an act of grave professional misconduct, which renders its integrity questionable;

d. has not entered into agreements with other suppliers aimed at distorting competition;

e. Is not subject to a conflict of interest within the meaning of regulation 24;

f. has not been involved in the preparation of this procurement procedure which would result in distortion of competition which could not be remedied by other, less intrusive, measures other than exclusion from this procedure;

g. has not had a contract terminated, damages or other comparable sanctions taken as a result of significant or persistent deficiencies in the performance of a substantive requirement under a prior public contract, a prior contract, or a prior concession contract as defined by the Concession Contracts Regulations 2016;

h. is not guilty of serious misrepresentation in providing any information required by this statement.

i. has not unduly influenced the decision-making process of the Authority or obtained confidential information that may confer upon it undue advantages in the procurement procedure;

j. in relation to procedures for the award of a public services contract, is licensed in the relevant State in which he is established or is a member of an organisation in that relevant State where the law of that relevant State prohibits the provision of the services to be provided under the contract by a person who is not so licensed or who is not such a member;

k. has fulfilled its obligations in the fields of environmental, social and labour law established by EU law, national law, collective agreements or by the international environmental, social and labour law provisions listed in the Public Contracts Directive as amended from time to time (as listed in PPN 8/16 Annex C).

I confirm that to the best of my knowledge my declaration is correct. I understand that the contracting authority will use the information in the selection process to assess my organisation's suitability to be invited to participate further in this procurement, and I am signing on behalf of my organisation. I understand that the Authority may reject my submission if there is a failure to provide a declaration or if I provide false or misleading information.

Organisation's name: Accenture (UK) Limited

Signed
(By Director of the Organisation or equivalent)

[Signature REDACTED]

Name: Mark Smith

Position: Managing Director

Date: 30th June 2021

Call-Off Schedule 10: Cyber Implementation Plan

Contract Title:	The Provision of a Defensive Information Warfare Platform
MOD Contract Number:	701570389 (DInfoCom/0188)
CSM Risk Acceptance Reference:	RAR-B3P283KU
CSM Cyber Risk Level:	High
Name of Supplier (to be shared with the MOD only):	Accenture UK Limited
Current Level of Supplier Compliance:	Cyber Essentials Plus (SAQ-429581742)
Reasons why Supplier is unable to achieve full compliance:	Full compliance confirmed by DCPP Team (full SAQ report and email confirmation submitted with bid)
Measures planned to achieve compliance/ mitigate the risk with associated dates:	Full compliance confirmed by DCPP Team (full SAQ report and email confirmation submitted with bid)
Anticipated date of compliance/mitigations will be in place:	Full compliance confirmed by DCPP Team (full SAQ report and email confirmation submitted with bid)
Current Cyber Essential Plus Certification No:	IASME-CEP-000775 (Expiry date: 05/09/2021) IASME-CEP-004473 (Expiry date: 05/07/2022)
Expiry Date:	As above
Renewal certification to be issued to the Authority:	Annually until expiration of the Contract
Name:	Eve Grisenthwaite
Position:	UK Government Security & Vetting Team Manager
Date:	20/07/2021

Call-Off Schedule 11: Monthly Statement of Work Template

Key Performance Indicators (TBA)

Service xxx – Sep 2021 Deliverables

				Days booked per role							
Ser	**Task**	**Description/Deliverable**	**Timescale**	**Role A**	**Role B**	**Role C**	**Days used**	**Completion**	**Benefits delivered**	**Cost of task**	**% completed**
1							**0**			**£0.00**	
2							**0**			**£0.00**	
3							**0**			**£0.00**	
				0	0	0	0			£0.00	

Signatures and Approvals

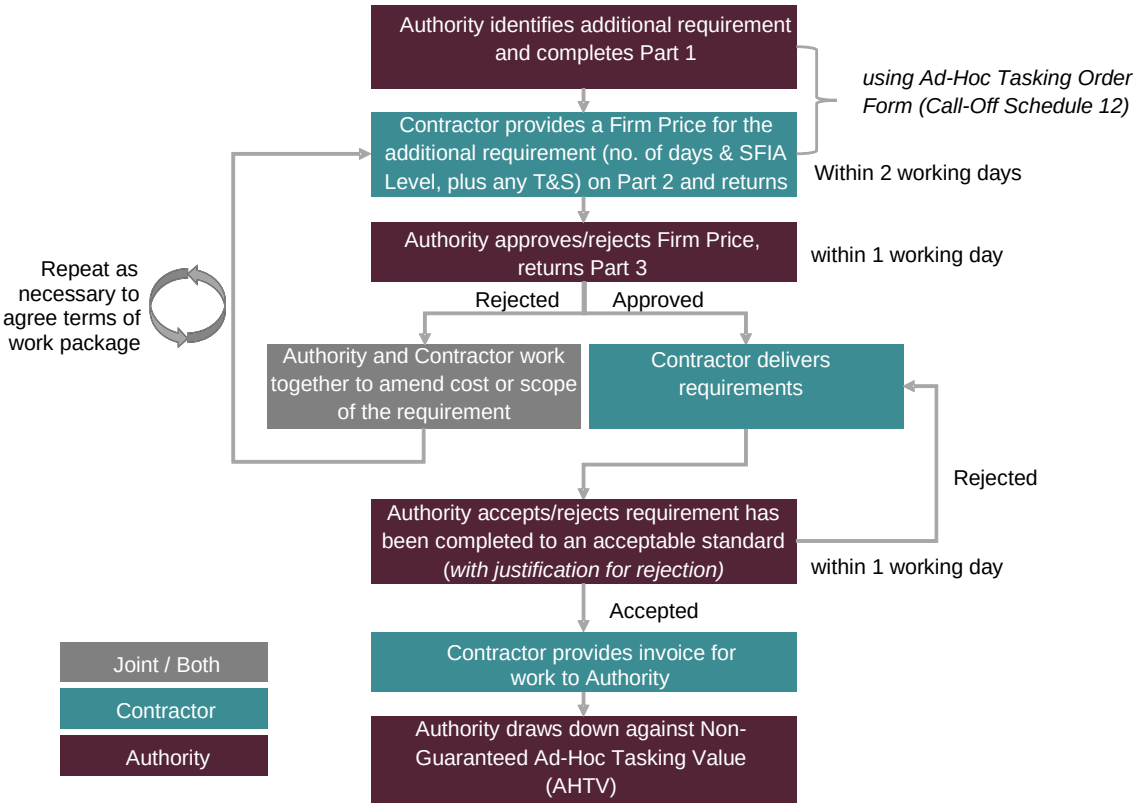
Agreement of this SOW

BY e-SIGNING this Statement of Work, the Parties agree that it shall be legally binding on the Parties:

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		**Signature:**	
Name:		**Name:**	
Role:		**Role:**	
Date:		**Date:**	

Call-Off Schedule 12: Tasking Order Process Map & Form

AD-HOC TASKING ORDER PROCESS MAP AND INFORMATION



Each Tasking Order is a MAXIMUM value and is to be based on the Firm Priced Man-Day Rates detailed at Call-Off Schedule 2.

Supplier to provide a detailed response on how they will deliver the outcome required.

No work shall commence until the Supplier is in receipt of the final Signed Tasking Order.

Once signed by all stakeholders the Authority will raise the necessary Purchase Order via CP&F. Upon completion of the Task and final invoices paid, the Authority will reduce (if necessary) the value of the Purchase Order to ensure unused funding is put back into the Non-Guaranteed Limit of Liability.

Due to the very nature of Ad-Hoc Tasking, Tasks can be cancelled at any time by the Authority. Amendments may be required which could extend the task on the basis that original technical re-quirement has not changed.

The Contract Terms and Conditions will support all Tasking Order Forms.

AD-HOC TASK ORDER FORM – PART 1

ORDER NUMBER: 001 (new number to be utilised for each additional Task)

CONTRACT No: 701570389 – DInfoCom/0188

TO: Accenture (UK) Limited

1. Please provide at PART 2 the details of the resources required to carry out the task described below.

2. TASK REQUIREMENT

To provide interim additional support to ……..……with effect from ……until……

Tasks to include (more details are provided within the attached Statement of Requirement (Where applicable)):

1)

2)

3. Detailed Tasks and timescales are to be agreed with SO3 Force Development. Accenture (UK) Limited are to report on a weekly basis to agree allocation of service priorities and risks in order to deliver services to meet contract requirements.

4. Resources: In accordance with the roles and rates within the Call-Off Schedule 2 with support to be provided from existing or additional Accenture (UK) Limited resources.

5. Payment will be based on the approved monthly Statement of Work between the customer and 6 (UK) Div. To Note: No T&S costs are to be included if work is to be undertaken at the usual place of work. Any T&S will be in accordance with the Authority's T&S policy, will be based on actual costs incurred and agreed with the Authority.

6. Accenture (UK) Limited are to complete PART 2 of this Tasking Order Form with proposed staffing profile (additional resource) and provide a detailed response on who they will deliver the outcome required.

7. LOCATION

8. PERIOD OF TASK……. subject to review thereafter.

SIGNATURE ……

NAME ……..…Authority's Customer

APPOINTMENT ……

CONTACT NO ……..….

AD-HOC TASK ORDER FORM – PART 2

ORDER NUMBER: 001 (new number to be utilised for each additional Task)

CONTRACT No: 701570389 – DInfoCom/0188

FROM: Accenture (UK) Limited

1. It is advised that Accenture (UK) Limited shall undertake the task detailed in PART 1 of this Order Form, within the timescale indicated, for the following MAXIMUM PRICE.

a.	List of roles and SFIA Level (as detailed in the Call-Off Order Form)	No of Days	Rate	Price
b.	Travel Expenses (if applicable)	No of Arisings	Rate	Price
c.	Total MAX FIRM PRICE for the task (a+b)	£		

SIGNATURE ……..….

NAME ……

APPOINTMENT ……..……..…

TELEPHONE NO: …….

DATE ……

AD-HOC TASK ORDER FORM – PART 3

ORDER NUMBER: 001 (new number to be utilised for each additional Task)

CONTRACT No: 701570389 – DInfoCom/0188

TO: Accenture (UK) Limited

1. To be completed by SO3 Force Development (or nominated representative)

DELETE EITHER A OR B AS APPROPRIATE

A. The Maximum price offer to undertake Order Number 001 on Contract No 701570389 – DInfoCom/0188 is commensurate with the work involved.

The work should proceed at ……Hours on……

B. The Maximum price offer to undertake Order Number 001 on Contract No 701570389 – DInfoCom/0188 is not commensurate with the work involved.

SIGNATURE ……

NAME ……

APPOINTMENT ……..……

TELEPHONE NO: ……..

DATE ……

2. In addition to the above confirmation, the following is to be completed by the Authority's Commercial Branch.

DELETE EITHER A OR B AS APPROPRIATE

A. The Maximum price offer to undertake Order Number 001 on Contract No 701570389 – DInfoCom/0188is accepted as an Ad-hoc Task.

B. The Maximum price offer to undertake Order Number 001 on Contract No 701570389 – DInfoCom/0188 is not accepted as an Ad-hoc task.

SIGNATURE ……

NAME

APPOINTMENT D Info Commercial

TELEPHONE NO: ……

DATE ……

Call-Off Schedule 13: Expenses Policy

UK Rail Travel

Standard Class must be selected.

Accommodation

Service Mess

If your business travel has taken you onto a base and you need overnight accommodation, it may be that staying in the Service Mess is more cost efficient than a hotel; and should be considered. All military personnel should refer to **JSP 752** Pt 2 Chapter 3 for occasions in which any other form of accommodation may be considered. For civilian staff, the availability and suitability criteria for Mess accommodation is being further developed and will be included in policy guidance shortly.

Hotel

All hotel bookings must be made using the **GBT Online Portal**.

Civilian staff must comply with the approvals processes (Chapter 2). Service Personnel must have both line management and budgetary written or verbal authority before making subsistence arrangements and should note that Night Subsistence (NS) is paid for an overnight absence where there is no suitable Service accommodation provision.

All staff must consult the MOD **capped hotel rates** for spend limits in each location. The Booking Service website will raise a warning if you select a hotel exceeding the capped rate. To proceed with such a booking, you must have line manager written approval of Band D/ OF2/OR7 or above (or locally delegated budget management staff).

Exceptional circumstances where you might exceed a cap rate include: the only hotel available; an overall saving; concern as a 'lone traveller'.

Travel & Subsistence

Spend taxpayers' money responsibly.

If in doubt about what to claim, seek advice from your line manager, budget manager, or from Unit HR/Admin Staff and/ or DBS – it is best to check before you commit to expenditure. Details for military personnel is in **JSP 752**, and for civilian staff in the **Policy Rules and Guidance**.

You cannot claim for alcohol purchased whilst undertaking business travel, either as part of a meal or consumed in isolation.

Subsistence cost limits: You can claim for actual receipted expenditure, within the subsistence limits detailed below, (**not** at a flat rate). You must obtain and retain itemised receipts for all claims. If you do not have a receipt you will need auditable line manager approval, e.g. by email, before you claim, and you must keep the approval.

Over 5 hours **£5.00**

Over 10 hours **£10.00**

Over 12 hours **£15.00**

Evening Meal **£22.50** (overnight stay)

Breakfast* **£10.00**

* *when not included in the hotel/B&B rate*

Motor Mileage Allowance (MMA) – UK

There are a number of different rates which are related to UK vehicle travel:

Motor Mileage Allowance (up to 10,000 miles)	30p per mile
• Motor Mileage Allowance (over 10,000 miles)	25p per mile
• Motorcycle	24p per mile
• Pedal cycle	15p per mile
• Passenger Supplement	3p per mile for first passenger; 2p per mile for second and additional passengers
• Equipment Supplement	2p per mile (taxable)
• Excess Fares Allowance	30p per mile

Home to Duty Liability

The Home To Duty Liability (HTDL) is the travel cost incurred getting to/from your normal place of work. This should be deducted from expenses incurred when undertaking business travel to/from the home and a business location. This deduction does not apply to travel between business locations.

Using a Private Vehicle is probably the easiest application. If you normally drive to work and use your vehicle for business travel, then your Motor Mileage Allowance claim should have a deduction commensurate with the normal mileage to work. So, if you normally travel 10 miles to/from your normal place of work (total 20 miles) and drive 30 miles to/from a

business location (total 60 miles), the claim should be reduced by 20 miles. This results in a net MMA claim of 40 miles. The deduction only applies to travel to/from the home and

business location; not between your normal workplace and business location(s).

Cyber Defence Services Supplement to Agreement for Purchase of Deliverables And/Or Services

Key Terms from the Security Cyber Defence Services Agreement for inclusion in the G-Cloud 12 Call-Off

3. Consent and Authorization.

The following definitions apply to this Agreement:

Access: means access, attempt to gain access to, collect, use, copy, monitor, move, connect, disconnect, intercept, modify, process, transfer and store.

Client Property: means computer systems; servers; technology infrastructures; telecommunications or electronic communications systems and associated communications; confidential information; data (including Client Personal Data, employee identification, authentication or credential data user details and other sensitive information); assets; devices; intellectual property; and/or physical premises, that are used by the Client, its Employees, customers, or suppliers, whether owned or otherwise controlled by the Client or owned by a third party.

Consents: includes all necessary consents, permissions, notices and authorizations necessary for Accenture to perform the Services, including any of the foregoing from Employees or third parties; valid consents from or notices to applicable data subjects; and authorizations from regulatory authorities, employee representative bodies or other applicable third parties.

Employee: means employees, contractors or other users under the control of the Client.

Personal Data means information relating to an identified or identifiable natural person.

The Client agrees and authorizes Accenture to:

a) do all acts as necessary for the performance of the Services, including:
   (i) Access Client Property;
   (ii) physically connect, disconnect, install, update, upgrade, manage and operate equipment, tools and software on Client Property;
   (iii) circumvent or overcome technology or physical measures designed to protect against unauthorized access to Client Property, including those that effectively control access to material protected by intellectual property laws, as well as use or provide technology to achieve any such circumvention;
   (iv) **intercept telecommunications and electronic communications;**
   (v) to the extent required to comply with law, share information or take such actions with respect to Client Property required by law enforcement authorities or regulatory authorities. In such cases Accenture will use reasonable endeavors to notify Client in advance, where it is permitted by such law enforcement and/or regulatory authorities to do so;

each as necessary for the performance of the Services set out in the applicable SOW;

b) retain for its business purposes any indicators of compromise, malware, anomalies, or other metadata (including or Client Personal Data that may be embedded in the same) found as part of, or related to the performance of the Services ("Metadata"). Accenture may analyze, copy, store, and use such Metadata in an aggregated, and de-identified manner.

While the Services may involve the simulation of malicious actors, the parties agree that the Services are being performed solely for the purposes of assessing and enhancing the effectiveness of Client's security; Accenture is performing the cyber defense Services at Client's request and has no intention of committing any civil or criminal offense. Client agrees that no act or omission of Accenture arising out of or related to Accenture's provision of the Services and Deliverables or compliance with law, will be deemed to exceed the authorization set forth above, be considered intentional misconduct or breach of the Agreement on the part of Accenture, or be construed by Client as a civil or criminal offence.

While Accenture uses reasonable care to carry out the Services in a manner designed to reduce the risk of damage to Client Property, Client acknowledges that there is inherent risk in the provision of security Services which may lead to operational degradation, performance impact, breach of Client's internal policies or industry standards, or otherwise impair Client Property and notwithstanding any other provisions in the Agreement to the contrary, Accenture will not be liable to Client or its employees or third parties for such damage, breach or impairment arising out of provision or receipt of the Services.

Client represents, warrants and agrees that:

(i) it has and will maintain all necessary rights, licenses, and Consents required to authorize Accenture to perform the Services, Access the Client Property, and provide the Deliverables;

(ii) it has full power and authority to, and the officer(s) or representative(s) executing this Agreement are authorized to bind Client to the terms and conditions hereof; and

(iii) Accenture is performing the Services in reliance on Client's representations, warranties and agreement set forth in this Section 3 and in the applicable SOW. As such, the performance of the Services shall not, on its own, be construed as intentional misconduct or breach of the Agreement on the part of Accenture.

Client shall be solely responsible for compliance with laws applicable to its business or the Services, including without limitation, any laws relating to network integrity or security or to data privacy or data protection ("Client Laws"). Accenture shall be authorized to act and rely upon any instructions provided by the Client. Accenture is not licensed or certified in any country, state, or province as a public accountant, auditor or legal advisor, or private investigator and is not being retained to provide accounting services, accounting guidance, audit or internal control advisory services, tax or legal advice or investigatory services that would require a license. Notwithstanding anything in the Agreement to the contrary, Client does not exclude or limits its liability (if any) to the Supplier for Client's breach of its representations, warranties or responsibilities set out in this Clause 3. This provision will survive the termination or expiration of the Agreement for any reason.

7. Warranties

Accenture warrants that its Services will be performed in a good and workmanlike manner, in accordance with this Agreement. Accenture will re-perform any work not in compliance with this warranty brought to its attention within thirty (30) days after that work is performed. Accenture further warrants that upon its execution, this Agreement will not materially violate any term or condition of any agreement that Accenture has with any third party and that the authorized representative(s) executing this Agreement are authorized to bind Accenture to the terms and conditions hereof. The preceding are the only warranties, and over-ride all other warranties, conditions and representations express or implied, including fitness for purpose, merchantability, non-infringement. Without limiting the generality or applicability of the foregoing, Accenture does not represent, warrant, or covenant that the services performed under this agreement will: (a) detect or identify all security or network threats to, or vulnerabilities of client's networks or other facilities, assets, or operations; (b) prevent intrusions into or any damage to client's networks or other facilities, assets, or operations; (c) return control of client or third party systems where unauthorized access or control has occurred; or (d) meet or help client meet any industry standard or any other requirements including the payment card industry data security standard.

10. Compliance.

(a) Compliance with International Trade Controls Laws. Each party shall comply with all export control and economic sanctions laws (collectively, "International Trade Control Laws") applicable to its performance under this Arrangement Letter, including the use and transfer of any products, software, technology or services subject to this Arrangement Letter (collectively, "Items"). Without limiting the foregoing, neither party shall transfer or cause the other party to transfer any Items: (i) to any country or region subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria, or the Crimea region of Ukraine); (ii) to any party in violation of applicable International Trade Control Laws; or (iii) that require government authorization to use or transfer without first obtaining: (a) the informed consent of the other party; and (b) the required authorization. (b) Anticorruption Laws. Each party acknowledges that it is familiar with and understands the provisions of the U.S. Foreign Corrupt Practices Act ("FCPA") and the U.K. Bribery Act of 2010 ("UKBA") and other applicable anti-corruption or anti-bribery laws ("AntiCorruption Laws") and agrees to comply with such laws.

'Application Security Testing and Application Penetration Testing Services'

1. The Deliverables are intended for Client's own internal use only and not intended for any use by third parties nor for use in any legal proceedings. Accenture disclaims any liability that may arise out of any third party's review and/or use of such Deliverables, whether in whole or in part and/or any liability arising out of or in connection with such Deliverables being used in legal proceedings. In no circumstances will Accenture be required to provide expert testimony in connection with the provision of the Services under this Agreement.

2. Client agrees that Accenture's performance of the Services will not constitute a breach of Client Policies.