Crown Commercial Service

Technology Services 2 Agreement RM3804/CCT540
Framework Schedule 4 - Annex 1

Final Order Form

In this Order Form, capitalised expressions shall have the meanings set out in Call Off Schedule 1 (Definitions), Framework Schedule 1 or the relevant Call Off Schedule in which that capitalised expression appears.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of the Call Off Contract for the duration of the Call Off Period.

This Order Form should be used by Customers ordering Services under the Technology Services 2 Framework Agreement ref. RM3804 in accordance with the provisions of Framework Schedule 5.

The Call Off Terms, referred to throughout this document, are available from the Crown Commercial Service website http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3804

Section A
General information

This Order Form is issued in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

Customer details
Customer organisation name ISS Commercial, Corporate Contracting Team (CCT)
Billing address Your organisation's billing address - please ensure you include a postcode [redacted]
Customer representative name The name of your point of contact for this Order [redacted]
Customer representative contact details Email and telephone contact details for the Customer's representative [redacted]

Supplier details
Supplier name The Supplier organisation name, as it appears in the Framework Agreement Centerprise International Limited

Crown Commercial Service

Supplier address
Supplier's registered address
Hampshire International Business Park, Lime Tree Way, Basingstoke, RG24 8GQ

Supplier representative name
The name of the Supplier point of contact for this Order
[redacted]

Supplier representative contact details
Email and telephone contact details of the supplier's representative
[redacted]

Order reference number
A unique number provided by the supplier at the time of the Further Competition Procedure
RM3804/CCT540

Section B
Overview of the requirement

Framework Lot under which this Order is being placed
Tick one box below as applicable (unless a cross-Lot Further Competition)

1. TECHNOLOGY STRATEGY & SERVICES DESIGN ☐
2. TRANSITION & TRANSFORMATION ☐
3. OPERATIONAL SERVICES (3c) ☒
4. PROGRAMMES & LARGE PROJECTS
   a. OFFICIAL ☐
   a. SECRET (& above) ☐

Customer project reference
Please provide a project reference, this will be used in management information provided by suppliers to assist CCS with framework management

RM3804/CCT540

Call Off Commencement Date

The date on which the Call Off Contract is formed – this should be the date of the last signature on Section E of this Order Form
19.01.2018

Call Off Contract Period (Term)
A period which does not exceed the maximum durations specified per Lot below:

Lot	Maximum Initial Term – Months (Years)	Extension Options – Months (Years)	Maximum permissible overall duration – Years (composition)
1	24 (2)	-	2
2	36 (3)	-	3
3	36 (3)	-	5
4	60 (5)	12 + 12 = 24 (1 + 1 = 2)	7 (5+1+1)

Call Off Initial Period Months
Estimated at 2 -3 months

Call Off Extension Period (Optional) Months
N/A

Crown Commercial Service

Minimum Notice Period for exercise of Termination Without Cause 30 days.
(Calendar days) *Insert right (see Call Off Clause 30.7)*

Additional specific standards or compliance requirements
Include any conformance or compliance requirements over and above the Standards (including those listed at paragraph 2.3 of Framework Schedule 2) which the Services must meet.
List below if applicable

DEFCON NO.	***Version***	***Description***
DEFCON 5J	***18.11.16***	***Unique Identifiers***
DEFCON 76	***12/06***	***Contractor's Personnel at Government Establishments***
DEFCON 522	***11/17***	***Payment and Recovery of Sums Due***
DEFCON 627	***12/10***	***QA requirement – Completion of Certificate of Conformity (CofC)***

Customer's ICT and Security Policy
Security Cleared personnel.

Security Management Plan
N/A

Section C
Customer Core Services Requirements

Services
As per the SOR provided (below), access to sites to follow the individual site process.

Tech services 2 – Lot3c - Technical Management

An End-to End Technical Service is required to provide assistance with the provision and remediation of Government infrastructure.

This service is required for a package of complex GFX works to support MOD GC/ IUS migration. The scope of the work is to deliver technical services and ensure the integrity of the infrastructure is maintained as well as the Electrical Certification of the equipment. This activity will encompass ensuring performance, capacity and availability of on-premise assets is maintained. This includes fixed devices and upgrading of power supplies/switches where necessary, along with associated remedial work. Electrical certification of NER equipment, (legal requirement) is part of the task. The preferred supplier will be required to enter Network Equipment Rooms and therefore must proactively plan, manage and deliver their own work schedule;by liasing with the Global Operations Security Control Centre (GOSCC) and working collaboratively with other stakeholders.

Crown Commercial Service

To assist we have provided below essential tasks which will require a technical service to ensure the current and future integrity of the ISS infrastructure for our customers.

Details are as follows:

Statement of Requirement for Services for Contract No RM3804/CCT540: Government Funded Equipment (GFX) to Support Global Connectivity (GC) and Integrated User Service (IUS) Programmes

2.1 Sample of works.

2.1.1 All works will be derived from authority requirements as detailed in 2.3.4.3. Works are described as, but not limited to:

2.1.2 Electrical Safety of Cabinets. Where the Supplier or Customer Authority identifies cabinets for project use that are deficient or not currently certified, the Contractor will undertake works to rectify any deficiencies (remedial effort) and provide the standard Institution of Engineering and Technology (IET) certification for power installation testing.

2.1.2.1 Identify associated racks to be powered off during a planned outage that supports implementation of works.

2.1.2.2 Carry out remedial action to raise cabinet to required standard.

2.1.2.3 Complete IET certification and submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing.

2.1.3 Additional Cabinet Power Sockets. Requirements for additional power will be met by installing new power sockets within the confines of a wall mounted or free standing cabinet. This may include replacing existing power bars with larger ones, fitting additional power bars or implementing a temporary solution using extension leads.

2.1.4 Enabling Works (remedial effort). There may instances of works that would be implemented by the Contractor e.g. installation of in-cabinet earthing bars, isolators and additional power forward of the NER isolator.

2.1.5 Additional Desk Top Power Sockets. Requirement for additional power will be met by installing new power sockets within 1.5m of new Hard Internet Protocol Telephones.

2.1.6 Provision of Cabinet. Where a new cabinet is required the Contractor will be requested to provide and implement the solution given in a Low Level Design or Migration Design Pack. The provision must meet the specification given within the design document and standards given in this contract.
2.1.7 New Containment. Installation of new fixed containment to the fabric of the building, which may include plastic or metal containment in accordance with the site design requirements.

2.1.8 Installation Designs. GFX installation designs to support the overarching ECR or Contractor ECR submission(s).

2.2 **Project Control**.

2.2.1 There are up to 166 IUS programme sites and 181 GC programme sites (plus an additional 225 PPS sites). These sites are under current Programme work-streams and are subject to Programme schedule change; additional sites may be included as new work-streams or Programmes are introduced.

2.2.2 The duration of consequential works for IUS is from Aug 17 to May 18 with GC already underway and scheduled for completion Oct 18. However note that both IUS and GC are subject to Programme project levelling.

2.2.3 Progress reports are to be submitted to the DaaP JPO (B) Site Readiness Team (SRT) group mailboxes on Mondays. GC and IUS are to have separate reports.

2.2.4 The Authority reserves the right to reduce/increase the number of sites in a tranche/phase.

2.2.5 The Authority reserves the right to substitute sites to ensure the overall project remains on schedule.

2.2.6 Cabinets are generally located within the Network equipment rooms on site. These tend to be secure air conditioned rooms for IT equipment only; smaller sites will have differing arrangements.

2.2.7 Predefined set of tests are stipulated in BS7671.

2.2.7.1 If the cabinet is physically or has electrical power connectivity to another cabinet or cabinets those cabinets must be tested as well. All cabinets should be on their own circuit and that should be identified. Where there is a shared circuit between cabinets that should also be identified. If information is not available, or the Contractor's engineers are unable to obtain information through visual inspection, the site would be treated on an exception basis with further action agreed between MoD and the Contractor.

2.2.8 Standards of work are to comply with BS7671, The Electricity at Work Regulations 1989, JSP 604 and ISSP 153.

2.2.9 The Contractor is responsible for booking the outage with the GOSCC and providing the necessary information required in accordance with ISSP 153. The Contractor is also responsible for meeting the requirements of DIO and CarillionAmey in regards to approval and clearance to work onsite.

2.2.9.1 The Contractor will gather electrical circuit information for the racks that will be affected by the outage. The Contractor will gather the information from the relevant authorised site representative where that information is available. Where there is a dependant cabinet that is detailed on provided documentation or visually identified to be on the same electrical supply, these will be noted and included in the outage notification. All Racks that are not directly connected either mechanically or electrically are not to be included in the testing process.

2.2.10 Site visits will require induction training prior to carrying out scope of works.

2.2.11 SC Clearance is required by those performing the work.

2.3 Site Engagement.

2.3.1 Introduction: The Information provided below defines the site activity process for implementation of GFX.

2.3.2 Scope: This process sets out the key elements and activities for site engagement, completing consequential works and Electrical safety testing of cabinets. It incorporates activities undertaken by the Customer Authority (CA) and the Contractor, as part of a joint approach.

2.3.3 Approach: The method for site engagement, completing consequential works and testing cabinets for electrical safety includes the following of a sequenced roll-out programme; on a site-by-site basis;

testing will be underpinned by all parties working collaboratively; testing will be planned to take place inside of the Working Hours except where there is a compelling and exceptional reason to undertake outside of normal working hours.

2.3.4 Overview:

2.3.4.1 The key process steps are set out below. Learning from Experience and continuous improvement will be applied throughout the process, using formal project review mechanism.

2.3.4.2 The purpose of this document to provide a process flow for the Customer Authority and the Contractor.

2.3.4.3 The Contractor will be provided the requirement by the SRT; this will usually be an extract from the Supplier Low Level Design or Migration Design Pack. Typical requirements are given in Para 2.1.

2.3.4.4 The Contractor is to release a Forward Work Schedule (FWS) and Risk & Method Statement (RAMS) to the SRT group mailbox. A Forward Work Schedule template will be provided to the Contract at contract award.

2.3.4.5 The SRT will Information Manage artefacts via their Group Mailbox(es) and notify the Customer Authority Regional Implementation Support Office (RISO) informing them of the scope and proposed date(s) of survey/works to assist the Contractor in gaining site access.

2.3.4.6 RISO will allocate an ISS Customer Manager (CM) to coordinate on-site activities through delivery of relevant artefacts to site point of contacts (POCs). The POCs will include, but not limited to, Security Officer (vetting/Access), Building Custodians, Health & Safety and SCIDA representatives. RISO will forward the FWS and RAMS to the CM who will facilitate the Contractor activity on-site.

2.3.4.7 The Contractor will attend site on agreed dates to complete surveys and/or to carry out consequential works.

2.3.4.8 Following Surveys the contractor will provide a firm price for works to the SRT Group Mailbox(es) on a site by site basic. The process flow at Para 2.6 refers.

2.3.4.9 Post approval (as per the process flow at Para 2.6), the Contractor will commence site works and gain necessary DIO and CarillionAmey approvals and clearance to undertake works on site. Where necessary, the Contractor will also arrange/coordinate the outage with the GOSCC.

2.3.4.10 The contractor is to notify the SRT via the Group Mailbox(es) on completion of site consequential works.

2.4 GFX Forecasted Volumes

2.4.1 Based upon current trends a site volume has been forecasted for GFX requirements across the GC and IUS projects.

2.4.2 The GC GFX requirements will be provided in batches with the first batch currently (noting that GFX status may change at contract award) consisting of 63 sites that have already been triaged. IUS and GC future batches will be submitted once designs have been triaged and the GFX identified, with the current forecast of an additional 222 sites requiring GFX.

Crown Commercial Service

2.4.3 The volume and frequency of GFX batches will be dependent upon triage and is only an estimation:

	Actual	Forecast	Total
GC UK	48	94	**142**
GC Overseas	15	24	**39**
IUS		104	**104**
	63	**222**	**285**

*Note: GFX requirements for the additional 225 GC PPS sites have not been included in the above forecast, but will be required as part of this framework.

NB: The additional sites are not applicable to this requirement and is provided for information purposes only.

Location/Site(s) for provision of the Services

List of sites

SID	Site Name	Site Contact	SRT Contact	Requirement
[redacted]	Rosyth Dockyard	[redacted]	[redacted]	Existing Cab ID: RACK 3 (MSC1100634) Location: BLDG 13 / GND FLR / NER. The current cabinet isolation switch is location inside the rear of the cabinet, this is not compliant and we require a new double pole lockable rotary isolator to be installed on a wall near the cabinet and labelled with the cabinet ID. Also within the cabinet we require an additional 12 way BS1363 PDU to be installed from one of the existing fused spur units at the top, rear of the cabinet. Complete IET certification for cabinets DIIF/DC1/RK1/R - BLDG 12/ LOWDEN / 1st FLR / RM FF46 / NER, DIIF/DC1/RK3/S - BLDG 12 / LOWDEN / 1st FLR / Rm FF46 / NER and RACK 3 (MSC1100634) - BLDG 13 / GND FLR / NER, DIIF/DC1/RK1/R - BLDG 15/ SYNCHRO / 1st FLR / NEC, l submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing.
[redacted]	Motherwell-Muir St TAC	[redacted]	[redacted]	Provide 1 x 4way 2U rack mounted (rear) PDU spur unit connecting to the existing DP Isolator. Reconnect both existing PDUs to individual Spur units on the PDU spur unit. Complete IET certification for cabinets DIIF/DC1/RK1/R - Main Bldg, G Flr, Elec Rm off Drill Hall, submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing.
[redacted]	Oakhanger NATO	[redacted]	[redacted]	New BS1363 PDU (Min 6 Way) required in DFT CCP/MISC CAB 3, Location: Bldg F4, Flr G, Control Rm as existing at capacity. There is a fused spur unit at the top rear of the cabinet which can be used to feed this new PDU. Complete IET certification for cabinets MISC - Bldg F4, Flr G, Control Rm 800 and DC1 RK1 - Bldg F4, Flr G, Rm Stairwell submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing.

[redacted]	Buchan-Remote Radar Head (RRH)	[redacted]	[redacted]	Bldg 39 (Red Rm) Sli Cabinet - Provide 1 x 1U 12 way C13 PDU at U07R connecting to spare spur unit on PDU spur unit at U41/42R.
[redacted]	St Athan RAF	[redacted]	[redacted]	Crypto cabinet (Location Building 145, Room 51 / SNER Cabinet ID: Crypto) a. Secure crypto cabinet to fabric of building. b. Update earthing arrangements within crypto cabinets to be JSP604 compliant. c. Move/replace SFS powering upper cabinet with a double pole rotary isolator in a more accessible location and insure it is labeled with cabinet ID. d. Complete IET certification for the following: 1. Cabinet ID: 0652DIIFRC00 & Cabinet ID: DII/DC1/RK00B/R CAB B Room: 30F / NER Building 145 2. Cabinet ID: Aux & Cabinet ID: SOC, Room: CCP Building: 151 3. Cabinet ID: SLi Wall Cabinet, Cabinet ID: Crypto (Pair of stacked 14u cabinets) & Cabinet ID: 0652DIIFSC00, Room: 51 / SNER Building: 145 Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO(B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. f. Any remedial works required to bring cabinet(s) to standard - must be compliant to JSP 604 Leaflet 4800.

[redacted]	Warminster DSG	[redacted]	[redacted]	There is presently a non-compliant cabinet installation inside Bldg 2J01 that needs to be brought up to JSP 604 standard to enable the site to be able to migrate. Namely the cabinet needs to be fitted to the fabric of the building, it needs to be earthed and needs to be fed from a DP rotary isolator switch. There is only one cab at present within Bldg 2J01 that houses the existing RLI active equipment. Complete IET certification for the cabinet. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.
[redacted]	Carnoustie-Barry Buddon Trng Range	[redacted]	[redacted]	15U Cabinet (MSC1100649) - Provide 1 x 4 way 2U rack mounted (rear) PDU spur unit connecting to the existing DP Isolator feeding this cabinet (Ensure Isolator is DP, if not replace as neccessary). Reconnect the existing PDU and the proposed new PDU to individual Spur units on the PDU spur unit. Provide 1 x 6 way BS1363 PDU mounted in rear of cabinet. This site has already been migrated but this work is required before ECR5 can be issued. Complete IET certification for the cabinet. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.
[redacted]	Upavon - Trenchard Lines	[redacted]	[redacted]	A additional vertically mounted 12 way BS1363 PDU is required within the rear of cab 1049DIIFRC01. This site has already been migrated but this work is required before ECR5 can be issued. Complete IET certification. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO(B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. All work iaw JSP 640.

		[redacted]		
[redacted]	York ACIO.108 Micklegate, York, YO1 6JX	[redacted]	[redacted]	ACIO/Rest Room, 15U Wall Cabinet, Cab DC1-RK1. Remove existing 6way BS1363 PDU and replace with 8way BS1363 PDU. Complete IET certification. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. All work iaw JSP 640.
[redacted]	Gosport DM	[redacted]	[redacted]	6 way BS1363 PDU is required in SC00 as existing at capacity, a temporary PDU has been installed within the cabinet for the migration. The Temp PDU needs to be permanently connected within the cabinet ensuring there is a single point of isolation for the cabinet. Complete IET certification for cabinet SC00. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.

[redacted]	RAF Moleswor th	[redacted]	[redacted]	In Building 326/Ground Floor/NER/Dennis Rack 05/01, remove the existing 12 way BS1361 PDU and the 5 way BS1361 (which is daisy chained from the first PDU). Replace with a new 20 way vertical PDU mounted in the rear of the cabinet, installed in accordance with JSP604/4800 Test and certify the following cabinets in accordance with regulations for Fixed Electrical Installations in accordance with IET 17th Edition Wiring Regulations, Amendment 3 as defined by BS 7671. Affix labelling to certified cabinet stating date of full test and and required next test date, label must be clear to define full test rather than visual inspection: Bldg 326/Gnd Flr/NER/Dennis Rack 05/01 CCP Node Room DFTS/CCP/BT ACM2 CCP Node Room DFTS/CCP/MISC Bldg 400, Gnd Flr Tech Control Room 1 FPI 150 Bldg 400, Gnd Flr Tech Control Rainford Cab 1702
[redacted]	London-Clifton Street TAC	[redacted]	[redacted]	1. THE EXISTING PDU AT THE REAR OF CABINET GC/OS-01 COVERS THE 19" RACK MOUNTING HOLES. IT WILL NEED TO BE MOVED DOWN BELOW 24U TO ALLOW THE INSTALLATION OF THE GC EQUIPMENT. 2. THERE IS A GFx REQUIREMENT FOR ADDITIONAL POWER IN CABINET GC/OS-01 TO SUPPLY THE GC EQUIPMENT. A NEW 12 WAY BS1363 PDU WILL BE REQUIRED. 3. THERE ARE TWO EARTH CABLES IN THE GC/OS-01 CABINET THAT HAVE BEEN CONNECTED TO A SINGLE POINT ON THE EARTH BAR, THESE NEED TO BE INDVIDUALLY CONNNECTED. 4. Complete IET certification for cabinet CABINET 8 in NER 1. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to

				site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.
[redacted]	Holbeach RAF	[redacted]	[redacted]	Install an additional 12Way C13 PDU into the rear of the Cab (Bldg 21\1st Flr \NER\DC1 RK1). There are 2 x spare fused spurs that are connected to the exiting 16Amp radial supply into the cabinet. Complete IET certification for cabinet Bldg 21\1st Flr \NER\DC1 RK1. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.
[redacted]	London-Horse Guards	[redacted]	[redacted]	1. A CLASS 3 CABINET IS TO BE INSTALLED WITHIN THE NER. SEPARATE CONTAINMENT IS REQUIRED BETWEEN THE NEW CABINET AND EXISTING CABINETS DC1 RACK 1 & DC1 RACK 3 2. THERE IS AN EXISTING, DECOMISSIONED CLASS 3 CABINET WITHIN THE OPS NER THAT NEEDS BE UTILISED FOR THIS INSTALLATION. 3. 16AMP SUPPLY FROM A DP ROTARY ISOLATOR FEEDING A 12 WAY BS1363 PDU TO BE INSTALLED. 4. A NEW FIBRE LINK IS REQUIRED BETWEEN CABINET DC1/RACK1 AND S-OPS-2. 5. Test and certify the following cabinets in accordance with regulations for Fixed Electrical Installations in accordance with IET 17th Edition Wiring Regulations, Amendment 3 as defined by BS 7671. Affix labelling to certified cabinet stating date of full test and and required next test date, label must be clear to

				define full test rather than visual inspection: Resited Class 3 cabinet (as above) Main NER Rack DC1/Rack 1 Main NER Rack DC1/Rack 3
[redacted]	RAF Honington	[redacted]	[redacted]	Building: 159, Room: MGR 2, Cabinet ID:TAFMIS/MSC1111555 Install 4 WAY C19 PDU into cabinet and connect to rotary isolator, existing PDU BS1363 to be be fed from a C19 socket. Install new 12 way BS1363 PDU this to also be fed from the new C19 socket. Instal to be JSP 604 compliant. Complete IET certification for cabinets, complete minor remedial action if required: Building: 159, Room: MGR 2,Cabinet ID:TAFMIS/MSC1111555, Building: 86A, Room: SERVER ROOM, Cabinet ID: RKY/R/MSC1111624, Building: 86a, Room: Server Room, Cabinet ID: RKZ/R/MSC1111621, Building: 86a, Room: Server Room,Cabinet ID: RKB/R/MSC1111620, Building 86a, Room: Frame Room, Cabinet ID: MSC1111546, Building 86a, Room: Frame Room, NEW CAB MSC1111546, Building 159, Room: MGR 2, Cabinet ID: TAFMIS/MSC1111555, Building 86a, Room: SNER, Cabinet ID: Sli/RK/CRYPTO/S/MSC1111542, Building 86a, Room: SNER, Cabinet ID: RKU/S/MSC1111628. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of

				completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.
[redacted]	Neatishead Remote Radar Head (RRH)	[redacted]	[redacted]	1. Install an additional 12 way BS1363 PDU into CAB ID: LDCN RACK A, Room: 2 BLACK NER located in building 58. 2. Install an additional 4 way BS1363 PDU to CAB ID: MSC1111674 Room: 1 Red NER located in building 58. Complete IET certification for cabinet: Building 68 Room:: 2 Black NER, CAB ID: LDCN Rack A, CAB ID: MSC1111708. Building 58 Room RED NER CAB ID: MSC1111670(CRYPTO), CAB ID: MSC1111675 Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.

[redacted]	Woodbridge Rock Barracks	[redacted]	[redacted]	CCS - Building: RHQ 2020 1st FLOOR Room: RED NER ROOM 120 Cabinet ID: SNER CABINET. Install 4 way C19 to be fed from a rotary isolator, remove all existing PDU's and replace with 2 x 12 way BS1363 PDU's fed from sockets from the newly installed C19 PDU. Install to be JSP 640 compliant. Complete IET certification for cabinets, complete minor remedial action if required. A full test of SNER CABINET required. For remaining cabinets "A Power on Test" is sufficient : Building: RHQ 2020 Gnd FLOOR, Room: BLACK NER ROOM 20, Cabinet ID: DIIF/UPS-DC2 CABINET 2 MSC1111876 & Cabinet ID:DIIF/DC1 CABINET 1 MSC1111877. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.
[redacted]	Feltham-Elmwood Ave	[redacted]	[redacted]	1. There is a requirement for a new 1000mm deep 42U cabinet at this site. The new cabinet has a requirement for diverse power for resilience. 2 x 12 way BS1363 PDU's fed from different supplies, these must have a single point of isolation (4 pole rotary isolator). 3. Complete IET certification for the new cabinet. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.

[redacted]	Rolls Royce	[redacted]	[redacted]	1. Install a Vertical PDU 6 x BS1363 to Building: DFTS POD Room: SERVER ROOM 4, Cabinet ID: MISC CABINET 3. 2. Inspect and conduct remedial work as required to bring the following CAB's to JSP 604 Leaflet 4800 standard: Building: DFTS POD, Room: Server Room 4, CAB ID: MISC CABINET 3, Cabinet ID: SSS COMMS 139, Cabinet ID: SSS Complete IET certification for the above CAB's and submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing.
[redacted]	Liverpool Walker House	[redacted]	[redacted]	1. Install a new C14, 12 Way PDU INTO Cab CCP/BT/AUX/CAB within Main Bldg CCP Room @ U9R, connected to the existing 4 way power distribution unit @ U1R/U2R. 2. Complete IET certification for cabinet CCP/BT/AUX/CAB. Submit the original and a soft copy to site and also submit a soft copy to MoD DaaP JPO (B) Site Readiness team. Completed certificates are required back to site within 5 days of completion of the testing. Works to be compliant to JSP 604 Leaflet 4800.

Crown Commercial Service

Additional Clauses *(see Annex 3 of Framework Schedule 4)*
Those Additional Clauses selected below shall be incorporated into this Call Off Contract

Applicable Call Off Contract Terms		**Optional Clauses** Can be selected to apply to any Order	
Tick any applicable boxes below		*Tick any applicable boxes below*	
A: SERVICES - Mandatory Lot 3 (Lot 4a + 4b where Lot 3 services are included)	☒	C: Call Off Guarantee	☐
A: PROJECTS - Optional Lots 1 and 2		D: Relevant Convictions	☐
A1: Testing	☐	E: Security Requirements (3,4,5,6&7 ISMS &SM Plan does not apply) Attached. Annex 1 (7&8 does not apply). Attached. Annex 2 applies. Attached. Annex 3 not required. SOR standards: To comply with BS 7671, the Electricity at Work Regulations 1989, JSP 604 (leaflet 4800) and ISSP153.	☒
A2: Key Personnel	☐	F: Collaboration Agreement *Where required please complete and append to this Order Form as a clearly marked document (see Call Off Schedule F)*	☐
B: SERVICES - Optional Lots 3 and 4a and 4b		G: Security Measures	☐
B1: Business Continuity and Disaster Recovery	☐	H: MOD Additional Clauses. (H5.1.3, H.5.1.4, H.5.1.5 & H.5.1.8 does not apply). Attached.	☒
B2: Continuous Improvement & Benchmarking	☐	**Alternative Clauses**	
B3: Supplier Equipment	☐	To replace default English & Welsh Law, Crown Body and FOIA subject base Call Off Clauses	
B4: Maintenance of the ICT Environment	☐	*Tick any applicable boxes below*	
B5: Supplier Request for Increase of the Call Off Contract Charges	☐	Scots Law Or	☐
B6: Indexation	☐	Northern Ireland Law	☐
B7: Additional Performance Monitoring Requirements	☐	Non-Crown Bodies	☐
		Non-FOIA Public Bodies	☐

Collaboration Agreement *(see Call Off Clause F)*

Crown Commercial Service

Organisations required to collaborate (Collaboration Suppliers) N/A	An executed Collaboration Agreement shall be delivered from the Supplier to the Customer within the stated number of Working Days from the Call Off Commencement Date *insert right* **OR** An executed Collaboration Agreement from the Supplier has been provided to the Customer and is attached to this Order Form. *tick box (right) and append as a clearly marked complete document*	Click here to enter text. ☐

Licensed Software Where Software owned by a party other than the Customer is used in the delivery of the Services list product details under each relevant heading below

Supplier Software	**Third Party Software**
N/A.	N/A. Include license or link in Call Off Schedule 3

Customer Property
Items licensed by the Customer to the Supplier (including any Customer Software, Customer Assets, Customer System, Customer Background IPR and Customer Data)
List below if applicable (see Call Off Clause 21)
N/A

Call Off Contract Charges and Payment Profile
Include Charges payable by the Customer to the Supplier (including any applicable Milestone Payments and/or discount(s), but excluding VAT) and payment terms/profile including method of payment (e.g. Government Procurement Card (GPC) or BACS)
List below or append as a clearly marked document (see Call Off Schedule 2)

Payment upon award of ECR5 for each site. Project Manager authority to receipt on confirmation of ECR5. Including actual receipts for T&S. T&S is an LOL.

Payment Profile			
Site	**Deliverable/T&S**	**Price (Ex-VAT)**	**Date**
Rosyth Dockyard	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Motherwell-Muir St TAC	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Oakhanger NATO	Labour, Materials, Certification	[redacted]	By 19 April 2018

	T&S	[redacted]	By 19 April 2018
Buchan-Remote Radar Head (RRH)	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
St Athan RAF	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Warminster DSG	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Carnoustie-Barry Buddon Trng Range	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Upavon – Trenchard Lines	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
York AC10.108 Micklegate	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Gosport DM	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
RAF Molesworth	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
London-Clifton Street TAC	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Holbeach RAF	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018

London-Horse Guards	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
RAF Honington	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Neatishead Remote Radar	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Woodbridge Rock Barracks	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Feltham-Elmwood Ave	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Rolls Royce	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018
Liverpool Walker House	Labour, Materials, Certification	[redacted]	By 19 April 2018
	T&S	[redacted]	By 19 April 2018

Undisputed Sums Limit (£)
Insert right (see Call Off Clause 31.1.1)

N/A

Delay Period Limit (calendar days)
Insert right (see Call Off Clause 5.4.1(b)(ii))

N/A

Estimated Year 1 Call Off Contract Charges (£)
For Call Off Contract Periods of over 12 Months

N/A

Enhanced Insurance Cover
Where a specific Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Schedule 14 please specify below

Third Party Public Liability Insurance (£)

Professional Indemnity Insurance (£)

Crown Commercial Service

Transparency Reports *(see Call Off Clause 23.4)*
If required by the Customer populate the table below to describe the detail (titles are suggested examples)

Title	Content	Format	Frequency
Order Form	All content except breakdown of prices by location and personal data.	PDF	Once

Quality Plans *(see Call Off Clause 7.2)*

Time frame for delivery of draft Quality Plans from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) N/A.
Where applicable insert right

Implementation Plan

Time frame for delivery of a draft Implementation Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) N/A
Where applicable insert right

BCDR *(see Call Off Clause B1)* N/A
An executed BCDR Plan from the Supplier is required prior to entry into the Call Off Contract *tick box (right) and append as a clearly marked complete document* ☐
OR

Time frame for delivery of a BCDR Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) N/A
Where applicable insert right

Disaster Period (calendar days) N/A

Supplier Equipment *(see Call Off Clause B3)*

B3 Applies B3.8 for default

X - Service Failures (number) *B3.8 for default*
Where applicable insert right

Y – Period (Months) *B3.8 for default*
Where applicable insert right

Key Personnel & Customer Responsibilities *(see Call Off Clause A2)*

	Customer Responsibilities
Key Personnel	[redacted]
Please supply a list of names of personnel employed on this task. (only staff that work on sites).	[redacted]

Crown Commercial Service

[redacted]

Relevant Conviction(s)
Where applicable the Supplier to include details of Conviction(s) it considers relevant to the nature of the Services.
List below or append as a clearly marked document (see Call Off Clause D where used)
No convictions.

Appointment as Agent *(see Call Off Clause 19.5.4)*
Insert details below or append as a clearly marked document

Specific requirement and its relation to the Services	Other CCS framework agreement(s) to be used
N/A	N/A

SERVICE LEVELS AND SERVICE CREDITS *(see Part A of Call Off Schedule 3)* *N/A*

Service Levels
If required by the Customer populate the table below to describe the detail (content is suggested examples)

Service Levels				
Service Level Performance Criteria	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	**Service Credit for each Service Period**
[Accurate and timely billing of Customer	Accuracy /Timelines	at least 98% at all times	[ ]	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure
Access to Customer support	Availability	at least 98% at all times	[ ]	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure
Complaints Handling	Availability/Timelines	At least 98% at all times	[ ]	0.5% Service Credit gained for each percentage under the specified Service

				Level Performance Measure
Provision of specific Services	Quality	at least 98% at all times	[ ]	2% Service Credit gained for each percentage under the specified Service Level Performance Measure
Timely provision of the Services [** hours a day, ** days a week.]	Services Availability	at least 98% at all times	[ ]	2% Service Credit gained for each percentage under the specified Service Level Performance Measure**]**

Critical Service Level Failure *(see Call Off Clause 9)* *N/A*
Agree and specify the metrics for Critical Service Level Failures in the marked areas below

In relation to **[specify the relevant Service Level]** a Critical Service Level Failure shall include a delay in producing **[specify the relevant Deliverable]** ordered by the Customer in excess of twenty four (24) hours more than once in any **[three (3) Month]** period or more than three (3) times in any rolling twelve (12) Month period.

In relation to **[specify the relevant Service Level]** a Critical Service Level Failure shall include a loss of **[specify the relevant Availability]** during core hours (08:00 – 18:00 Mon – Fri excluding bank holidays) to the **[specify the relevant Service]** for more than twenty four (24) hours accumulated in any **[three (3) Month]** period, or forty eight (48) hours in any rolling twelve (12) Month period.

The number of Service Level Performance Criteria for the purpose of Call Off Clause 8.6 shall be **[specify number]**.

Service Credits N/A
Formula for calculation

x% (Service Level Performance Measure) - **x**% (actual Service Level performance)	=	**x**% of the Call Off Contract Charges payable to the Customer as Service Credits to be deducted from the next Valid Invoice payable by the Customer
Worked example:		
98% (e.g. Service Level Performance Measure requirement for Service Level Performance Criterion of accurate and timely billing to Customer) - 75% (e.g. actual performance achieved against this Service Level Performance Criterion in a Service Period)	=	23% of the Call Off Contract Charges payable to the Customer as Service Credits to be deducted from the next Valid Invoice payable by the Customer

Service Credit Cap N/A
Agree and specify the Service Credit Cap in the marked areas below

In the period from the Call Off Commencement Date to the end of the first Call Off Contract Year **[xxx]%** of the Estimated Year 1 Call Off Contract Charges; and

Crown Commercial Service

during the remainder of the Call Off Contract Period, **[xxx]**% of the Call Off Contract Charges payable to the Supplier under this Call Off Contract in the period of twelve (12) Months immediately preceding the Month in respect of which Service Credits are accrued.

Additional Performance Monitoring Requirements N/A

Technical Board *(see paragraph 2 of Call Off Schedule B7)* – where required

If required by the Customer populate the table below to describe the detail

Required Members			
Job Title	**Name**	**Location**	**Frequency**

Time frame in which the Technical Board shall be established – from the Call Off Commencement Date (Working Days) *Where applicable insert right* Click here to enter text.

Section D
Supplier response

Suppliers - use this section to provide any details that may be relevant in the fulfilment of the Customer Order

Commercially Sensitive information

Any information that the Supplier considers sensitive for the duration of an awarded Call Off Contract

[redacted]

Total contract value

Please provide the total contract value (for the Call Off Initial Period) as detailed in your response to the Customer's statement of requirements

£19,152.89 (Ex VAT) ([redacted])

Crown Commercial Service

Section E
Call Off Contract award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of this Order Form and the Call Off Terms (together referred to as "the Call Off Contract") for the duration of the Call Off Contract Period.

SIGNATURES

For and on behalf of the Supplier

Name	[redacted]
Job role/title	**Director, Defence and Security**
Signature	[redacted]
Date	**22/01/18**

For and on behalf of the Customer

Name	[redacted]
Job role/title	**ISS Comrcl D 13**
Signature	[redacted]
Date	**22/01/18**

Crown Commercial Service

Optional Clauses: E Security Requirements:

E. SECURITY REQUIREMENTS

E.1 This Clause shall apply if so specified in section C of the Order Form.

E.2 The Supplier shall comply with the Security Policy and the requirements of Call Off Schedule E (Security) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

E.3 The Customer shall notify the Supplier of any changes or proposed changes to the Security Policy.

E.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Services it may propose a Variation to the Customer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Call Off Contract Charges shall then be subject to the Variation Procedure.

E.5 Until and/or unless a change to the Call Off Contract Charges is agreed by the Customer pursuant to the Variation Procedure the Supplier shall continue to provide the Services in accordance with its existing obligations.

CALL OFF SCHEDULE E: SECURITY

1. DEFINITIONS

1.1 In this Call Off Schedule E, the following definitions shall apply:

"Baseline Security Requirements"	means those requirements outlined in Annex 1 of this Call Off Schedule E
"Breach of Security"	means the occurrence of: a) any unauthorised access to or use of the Services, the Sites, the ICT Environment and/or any ICT, information or data (including the Confidential Information and the Customer Data) used by the Customer and/or the Supplier in connection with this Call Off Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Customer Data), including any copies of such information or data, used by the Customer and/or the Supplier in connection with this Call Off Contract, in either case as more particularly set out in: (1) the Baseline Security Requirements in Annex 1 to this Call Off Schedule E; and

	(2) the Security Policy in Annex 2 to this Call Off Schedule E.
"ISMS"	the information security management system developed by the Supplier in accordance with paragraph 2 (ISMS) as updated from time to time in accordance with this Call Off Schedule E;
"Security Policy Framework"	the HMG Security Policy Framework https://www.gov.uk/government/publications/security-policy-framework; and
"Security Tests"	has the meaning given in paragraph 6.1 of this Call Off Schedule E (Testing of the ISMS).

2. INTRODUCTION

2.1 The Parties acknowledge that the purpose of the ISMS and the Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Call Off Contract will be met.

2.2 The Customer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.3 Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security.

2.4 The Supplier shall use as a minimum, Good Industry Practice, in the day to day operation of any system holding, transferring or processing Customer Data and any system that could directly or indirectly have an impact on that information, and shall ensure that the Customer Data remains under the effective control of the Supplier at all times.

2.5 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and system and on request shall supply this document as soon as practicable to the Customer.

2.6 The Customer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Customer's security provisions represents an unacceptable risk to the Customer requiring immediate communication and co-operation between the Parties.

3. ISMS - DOES NOT APPLY

4. SECURITY MANAGEMENT PLAN – DOES NOT APPLY

5. AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN – DOES NOT APPLY

6. TESTING OF THE ISMS – DOES NOT APPLY

7. COMPLIANCE OF THE ISMS WITH ISO/IEC 27001 AND ISO/IEC 27002 – DOES NOT APPLY

8. BREACH OF SECURITY

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 8.1 of this Call Off Schedule, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Customer) necessary to:

(a) minimise the extent of actual or potential harm caused by any Breach of Security;

(b) remedy such Breach of Security or any potential or attempted Breach of Security or protect the integrity of the ISMS against any such Breach of Security or any potential or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Service Level Performance Measures, the Supplier shall be granted relief against any resultant under-performance for such period as the Customer, acting reasonably, may specify by written notice to the Supplier;

(d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure;

(e) supply any requested data to the Customer or the Computer Emergency Response Team for UK Government ("GovCertUK") on the Customer's request within two (2) working days and without charge (where such requests are reasonably related to a possible incident or compromise); and

8.2.2 as soon as reasonably practicable provide to the Customer full details (using such reporting mechanism as defined by the ISMS) of the Breach of Security or the potential or attempted Breach of Security, including a root cause analysis where required by the Customer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy or Baseline Security Requirements or the requirements of this Call Off Schedule, then any required change to the ISMS shall be at no cost to the Customer.

9. VULNERABILITES AND CORRECTIVE ACTION

9.1 The Customer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Customer's information.

9.2 The severity of threat vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Customer; or

9.3.3 the Customer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Supplier Solution and Implementation Plan shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be upgraded within 6 months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such Supplier COTS Software and Third Party COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 months of release of the latest version ; or

9.4.2 is agreed with the Customer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Call Off Contract Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the Customer within five (5) Working Days of the end of each month detailing

both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

9.5.8 inform the Customer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Customer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Notifiable Default, and the Supplier shall comply with the Rectification Plan Process.

Optional Clauses: E Security Requirements, Annex 1:

1. HIGHER CLASSIFICATIONS

1.1 The Supplier shall not handle Customer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Customer.

2. END USER DEVICES

1.2 When Customer Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

2.1 Devices used to access or manage Customer Data and services must be under the management authority of Customer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Customer. Unless otherwise agreed with the Customer in writing, all Supplier devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2).
Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Customer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Customer.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

3.1 The Supplier and Customer recognise the need for the Customer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Customer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Customer Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Customer in advance where the proposed location is outside the UK. Such approval shall not be unreasonably withheld or delayed unless specified otherwise in this Agreement and provided that storage, processing and management of any Customer Data is only carried out offshore within:

3.2.1 the European Economic Area (EEA);

3.2.2 in the US if the Supplier and or any relevant Sub-contractor have signed up to the US-EU Safe Harbour Agreement; or

3.2.3 in another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the EU Commission.

3.3 The Supplier shall:

3.3.1 provide the Customer with all Customer Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Customer Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Customer Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Customer Data held by the Supplier when requested to do so by the Customer.

4. NETWORKING

4.1 The Customer requires that any Customer Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

4.2 The Customer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY ARCHITECTURES

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Customer Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. PERSONNEL SECURITY

6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Customer Data.

6.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Customer Data except where agreed with the Customer in writing.

6.4 All Supplier Personnel that have the ability to access Customer Data or systems holding Customer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Customer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Sub-Contractors grants increased ICT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7 IDENTITY, AUTHENTICATION AND ACCESS CONTROL – DOES NOT APPLY

8 AUDIT AND MONITORING – DOES NOT APPLY

Optional Clauses: E Security Requirements, Annex 2:

ANNEX 2: SECURITY POLICY

Adhere to individual MOD Sites security policy when undertaking SOR activities.

H. MOD ADDITIONAL CLAUSES

H.1. This Clause H shall apply if so specified in section C of the Order Form.

H.2. The definition of Call Off Contract in Call Off Schedule 1 (Definitions) to the Call Off Terms shall be replaced with the following:

"Call Off Contract" means this written agreement between the Customer and the Supplier consisting of the Order Form and the Call Off Terms and the MoD Terms and Conditions.

H.3. The following definitions shall be inserted into in Call Off Schedule 1 (Definitions) to the Call Off Terms:

"MoD Terms and Conditions" means the contractual terms and conditions listed in Schedule H which form part of the Call Off Terms

"Site" shall include any of Her Majesty's Ships or Vessels and Service Stations.

"Officer in charge" shall include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Officers superintending Government Establishments.

H.4. The following clauses shall be inserted into Clause 2 of this Call Off Contract (Due Diligence):

H.4.1 The Supplier confirms that it has had the opportunity to review the MoD Terms and Conditions and has raised all due diligence questions in relation to those documents with the Customer prior to the Commencement Date.

H.4.2. Where required by the Customer, the Supplier shall take such actions as are necessary to ensure that the MoD Terms and Conditions constitute legal, valid, binding and enforceable obligations on the Supplier.

H.5. ACCESS TO MOD SITES

H.5.1. In this Clause H.5:

H.5.1.1 The Customer shall issue passes for those representatives of the Supplier who are approved for admission to the Site and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Customer and shall be surrendered on demand or on completion of the supply of the Services.

H.5.1.2 The Supplier's representatives when employed within the boundaries of a Site, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force for the time being for the conduct of personnel at that Site. When on board ship, compliance shall be with the Ship's Regulations as interpreted by the Officer in charge. Details of such rules, regulations and requirements shall be provided, on request, by the Officer in charge.

H.5.1.3 Does not apply

H.5.1.4 Does not apply

H.5.1.5 Does not apply

Crown Commercial Service

H.5.1.6 Accidents to the Supplier's representatives which ordinarily require to be reported in accordance with Health and Safety at Work etc Act 1974, shall be reported to the Officer in charge so that the Inspector of Factories may be informed.

H.5.1.7 No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Supplier's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current Ministry of Defence rates.

H.5.1.8 Does not apply