Council of Reserve Forces' and Cadets' Associations (CRFCA)

Invitation to Tender

Lot 1 - Managed Services Provider

Lot 2 - Wide Area Network Services

1. Introduction

1.1   This Invitation to Tender ('ITT') provides information for consideration with respect to the detailed requirements of the Council of Reserve Forces' and Cadets' Associations ('CRFCA') described below. This procurement process commenced with the publication of the related Official Journal of the European Union contract notice.

1.2   This ITT has been prepared by CRFCA for use by those Tendering for the Contract ('Tenderers'), their professional advisers, and other parties essential to preparing the Tender for the Contract and for no other purpose.

1.3   The ITT will be managed as a formal process and will be accompanied by other due diligence activities to confirm the services supplier (the "Supplier").

1.4   Unless the context requires otherwise, words in the singular shall include the plural and in the plural shall include the singular.

1.5   Any words following the terms including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

1.6   Tenderers are required to answer all applicable questions and include all documentation requested. The response must be completed in English.

1.7   Original documents must not be included as CRFCA does not accept responsibility for their return.

1.8   All information received in connection with this ITT will be treated in the strictest confidence. All communications will be treated as commercially confidential.

1.9   The ITT response shall be submitted on the basis that any offer within it shall remain in force for a minimum of six months from the date fixed for the submission of responses.

1.10   No alteration to the successful Tenderers position post award of the Contract will be accepted, unless this is due to external factors beyond the control of the Tenderer, is acceptable to CRFCA and is in accordance with any applicable legislation.

1.11   ITT responses must be submitted in accordance with the following instructions. Any response not complying fully with any of the instructions in this document may be rejected by CRFCA, whose decision in the matter shall be final.

1.12   ITT responses shall only be submitted on the basis that they are bona fide competitive tenders. It is to be agreed that CRFCA shall have the power to cancel the contract and to recover from the Tenderer the amount of any loss arising from the cancellation if either the Tenderer:

a)   Shall have offered or given or agreed to give any officer or member of CRFCA staff any gift or consideration of any kind as an inducement or bribe to influence its decision in the tendering procedure. The word "Tenderer" for these purposes shall be deemed to include any and all persons employed by the Tenderer, or who are purporting to act on the Tenderer's behalf whether the Tenderer is aware of their acts or not, or

b)   Shall have communicated to any other person than CRFCA the amount or approximate amount of the proposed tender other than in confidence in order to obtain quotations necessary for the preparation of the tender, or for insurance purposes, or

c)   Shall have entered into any agreement or arrangement with any person as to the amount of any proposed tender or that person shall refrain from tendering.

1.13   The Tenderer shall be responsible for obtaining all information necessary for the preparation of its response and all costs, expenses and liabilities incurred by the Tenderer in connection with the preparation and submission of the response shall be borne by the Tenderer.

1.14   CRFCA shall not be bound to accept any response submitted and reserves the right to accept any response either in whole or in part or not at all.

1.15   CRFCA reserves the right to cancel this ITT process at any point. In the event that CRFCA cancels the ITT process CRFCA shall not be liable for any costs resulting from the cancellation or for any other costs incurred by Tenderers.

1.16   Tenderers must satisfy themselves of the accuracy of any information provided by CRFCA. CRFCA accepts no responsibility or liability whatsoever for any loss or damage of whatever kind and howsoever caused arising from or in consequence of the use by Tenderers of such information.

1.17   Tenderers shall take appropriate steps to ensure that neither they or their staff are placed in a position where, in the reasonable opinion of CRFCA, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Tenderer and the duties owed to CRFCA. The Tenderer will disclose to CRFCA full particulars of any such conflict of interest which may arise, via a formal email or written notification.

1.18   The reproduction of this ITT by electronic, photographic or other means is permitted only for the sole purpose of preparing the Tenderers response to the ITT.

1.19   All documentation provided with this ITT referring to details of equipment lists, user numbers, sites to be supported, etc. reflects the position as at the date of this ITT. CRFCA reserve the right to modify this information prior to final contract, to reflect any changes in the estate that might take place prior to that point.

1.20   All times listed within this ITT are local UK times.

2. Background and Requirements

2.1 Background Information; CRFCA

The hyperlink below can be used to locate further information regarding CRFCA:

https://www.gov.uk/government/organisations/reserve-forces-and-cadets-associations/about

This ITT relates to the proposed CRFCA project to review the provision of Information and Communication Services (Managed Services Provider) and Wide Area Network Services (WAN Services) to the organisation.

2.2 Overview of Requirements – Lot 1, Managed Service Provider

CRFCA is seeking to appoint a Managed Services Provider (MSP) to manage and support the Communication & Information Systems for CRFCA Head Office staff; for the 13 Reserve Forces' and Cadets' Associations (RFCAs); the approximately 55 County Army Cadet Force organisations (ACF); and their users. The service will also support CRFCA's obligation to deliver their Service Level Agreement (SLA) commitment to the UK Ministry of Defence (MOD).

The IT systems to be supported include a data centre in Aldershot, with back up facilities in a CRFCA owned data centre in London; core systems including "Project Haldane 2" (PH2); local area networks; firewalls and local IT systems in the RFCAs and around 1000 mobile devices, consisting of laptops, mobile phones, printers, etc. The MSP will also be responsible for support of the Wide Area Network (WAN) that is provided under Lot 2.

As the RFCAs are arm's length bodies to the MOD, and because they work mostly with the civilian stakeholders in delivering their commitments, the core PH2 system is designed to straddle the MOD systems and the Internet. It is believed to be a unique system of its kind, and therefore needs a level of security that assures the MOD of protection against internet based cyber threats. All staff involved in the delivery of the service must have security clearance to at least SC level. See https://www.gov.uk/government/collections/national-security-vetting for further information.

PH2 is accredited by the MOD through the Defence Assurance and Information Security (DAIS) team to hold information assets up to the Protective Marking of OFFICIAL-SENSITIVE. Any location where information is managed by the MSP as part of delivering the service will have to be accredited by DAIS. (See https://www.gov.uk/guidance/defence-security-and-assurance-services-defence-industry-list-x for further information). Please note that list X status is not a requirement for this tender.

The service must be managed by a Single Point of Contact incident management facility that provides the ability to log incidents by telephone, web or email, with service hours of 8am to 6pm, Monday to Friday, with additional service support 6pm to 10pm Monday to Friday and on Saturdays from 8am to 6pm. All processes used in the delivery of the service must be ITIL compliant.

2.3 Overview of Requirements – Lot 2, WAN support

In addition to the MSP role, CRFCA is also seeking to appoint a contractor to provide the WAN infrastructure, network devices and support for the CRFCA, the RFCAs and the ACFs. Details of the network and support requirements are provided within this document.

3. Administration

3.1   ITT Contacts

CRFCA are working with eXceeding to administer this ITT process.

All issues relating to this ITT, either administrative or technical, should be addressed to:

CRFCA@exceeding.uk.com

All Tenderers are required to use the above email address for all project correspondence; no direct contact is to be made with CRFCA throughout the duration of the ITT process.

3.2   ITT Timetable

A high-level summary of the ITT timetable is shown below.

Release of the ITT	*10.12.2018*
Final deadline for submission of questions	*21.01.2019 @ 12:00 Hours*
Responses to questions provided by	*04.02.2019 @ 12:00 Hours*
Closure date for ITT responses (including Supplier Questionnaire)	*05.03.2019 @ 12:00 Hours*
ITT evaluation period	*06.03.2019 through to 01.04.2019*
Interviews and presentations	*Interviews and presentations will be held during April 2019.* *Exact timings will be advised at a later date.*
Selection Dates	*To be confirmed.*

It is requested that Tenderers advise CRFCA of their intention to respond to this ITT by *21.01.2019 @ 12:00 Hours*. Any questions relating to the ITT must be submitted before *21.02.2019* @ 12:00 hours. Questions submitted after this date will not be answered.

The closure date for the receipt of responses is *05.03.2019* @ 12:00 hours. Responses received after this time will not be considered. If any Tenderer believes that this target is unrealistic, they should contact "*CRFCA@exceeding.uk.com*" within 5 working days of the release of this ITT, detailing the issue(s) which they have identified. Should the identified issues be judged as valid by CRFCA, an extension will be agreed for all the Tenderers participating in the ITT process.

CRFCA will evaluate ITT responses in the period between *06.03.2019* and *01.04.2019*. It is expected that interviews and presentations will take place in April 2019, sufficient notice will be provided to Tenders to facilitate their participation in these activities.

3.3   ITT Submission

Tenderers are required to submit their response to the Suppliers Questionnaire (SQ) and this ITT in an electronic format as instructed in this ITT. Answers to questions should contain no more than 250 words, unless otherwise specified.

For the avoidance of doubt, please note that acceptable formats for submission are:

- Microsoft Word 2010, or later, where required.
- Microsoft Excel 2010, or later, where required.

Documents submitted in pdf format, other than where specifically requested, are not acceptable and will not be reviewed. Hyperlinks or embedded images must not be included in responses and will not be reviewed if they are included.

Responses to this ITT should include "CRFCA ITT – Managed Services Provider", or "CRFCA ITT – WAN Provider" in the subject line and ONLY be emailed to:

CRFCA@exceeding.uk.com

Responses to the ITT must include a completed Supplier Questionnaire (SQ) for each Lot that the Tenderer is responding to (see Appendices A and B) along with a completed Supplier Response using the Microsoft Excel template provided in Appendix L (Lot 1 - Managed Service Provider) and / or Appendix M (Lot 2 - WAN service). Failure to include a completed SQ will exclude the supplier from the evaluation for the relevant Lot.

The final closure date for responses is *05.03.2019* @ 12:00 hours local UK time. Any ITT response received after this date and time will not be considered. If rejected for late delivery, the Tenderer will be notified of this fact and no details within such responses shall be recorded or disclosed.

3.4   Questions and Answers

All questions, requests for clarification or advice and the responses provided by CRFCA will be circulated to all Tenderers.

As a matter of course, the identity of the enquirer will be protected. Where a Tenderer views any query as confidential (particularly where it believes that the release of the query to other Tenderers may reveal commercially sensitive or confidential information or a trade secret) the following procedure will be adopted:

1. If a Tenderer believes that a query is of a confidential or commercially sensitive nature, then it must be marked as such.
2. If CRFCA considers, in its absolute discretion, that it is able to treat the query on a confidential basis, then it will do so.
3. If CRFCA considers, in its absolute discretion, that it is unable to treat the query on a confidential basis having regard to current guidance and legislation, then it will notify the Tenderer of its decision and the Tenderer will have the opportunity to withdraw the query; and
4. If the Tenderer does not withdraw the query then the query and its answer will, where appropriate, be released to all potential Tenderers.

3.5   Confidentiality

Information in this ITT and all discussions and correspondence between Tenderers and CRFCA staff shall be treated as confidential.

Tenderers shall not disclose or publish to any third party for any reason, without prior written consent from CRFCA.

The name of CRFCA or any other identity must not be used for advertising or for publicity, under any circumstances.

3.6   Required Response Content

All Tenderers should supply the information requested in this ITT in the format requested, including a completed Supplier Questionnaire (SQ) and a Supplier Response for the Lot(s) that they are submitting a response to. Should any Tenderer be unable to provide a response to any particular item, a clear statement must be included detailing the reason for the omission. The SQ response must be in the format provided in Appendix A for Lot 1 (MSP) and Appendix B for Lot 2 (WAN). The Supplier Response to questions raised in this ITT must be provided using the Microsoft Excel template in Appendix L (Lot 1 - MSP) or Appendix M (Lot 2 -WAN).

3.7   Next Steps

Following the ITT submission, successful Tenderers will be invited to participate in the subsequent stage, which will involve presentations and detailed discussions regarding project objectives, timescales and implementation.

4. Service Requirements

The following paragraphs, along with the Appendices included with the ITT, provide an overview of the services to be provided in each Lot.

4.1 Lot 1 – Managed Service

Lot 1 is for a Managed Service contract to support the IT estate for the CRFCA, the Reserve Forces and the Cadet Associations, including data centre based systems, local IT systems and mobile devices (laptops, mobile phones, etc.).

Overview of Requirements:

The following items are in scope of the managed services contract:

- Hardware including servers, PCs, laptops, printers, network elements including firewalls, mobile devices (including phones) and telephony. A full list of current equipment to be supported within the scope of the contract is provided in Appendix D
- Services at the contracted sites, including the CRFCA Head Office, the primary data centre (located in Aldershot), back up facilities (based in a CRFCA owned data centre in London), ACF County HQs, remote users and the RFCAs. The sites to be covered by the contract are listed in Appendix E
- Support and maintenance of the CRFCA Local Area Networks (LAN) in the data centres and CFRCA sites (head office and remote)
- Operating Systems (OS) (Windows and Linux)
- DNN Application Software (Web Sites)
- SQL Server Databases
- Microsoft SharePoint Server and configuration
- Microsoft Active Directory (AD)
- Microsoft Internet Information Service (IIS)
- Microsoft Exchange Mail Services
- MS Office Applications
- Public Calendars (available within the Intranet only)
- Sage HR
- Log 360 – Audit software
- Controlpoint – SharePoint audit software
- Centralised Patching
- Hardware Audits
- Management Systems
- Software Distribution System
- Skype for Business
- SPOC Helpdesk and system management Software
- User Access Control (UAC) software
- Asset Management Software
- Remote users' connections software and routing to data

- Mobile Device Management (MDM) using the MobileIron software suite
- Symphony estates and accounting software, provided by Software Factory Ltd (SFL)
- Port based Network Access Control (PNAC)
- PH2 Web Applications (some PH2 applications are available as Web Applications in PH2E without using the virtual desktops in PH2)
- Watchguard Firewalls
- Support of the Eracent software installed on RLI based assets
- Management of the WAN
- Applications needed in support of the service (e.g. Anti-Virus Software)
- Security of data (provision of software & user access levels)
- Maintenance of all supported hardware and software
- Disaster Recovery and Backup Services.

Infrastructure Overview:

The infrastructure to be supported by this contract is called "Project Haldane 2 (Extended)" (PH2E). Within the PH2E infrastructure, there is also a separate closed network called PH2 which does not allow external connection to the internet. The PH2E private cloud is hosted on 3 physical hosts and a SAN, whilst the wider network comprises 71 Virtual Servers, a number of physical servers and back up devices such as Network Attached Storage (NAS), SAN and back-up tape drives. There are over 1000 user devices, printers, scanners and franking machines connected to the network. There are 75 sites in the network each of which has their own local domain controller, connected by VPN. The local domain controllers also fulfil the roles of file server, print server and DNS. This is a closed network with only one gateway to the internet.

The closed PH2 network has a large number of local area networks that are joined by VPNS to form the Intranet. In addition to the PH2E equipment outlined above, PH2 includes 55 virtual servers managed by one V Centre; 5 domain controllers; 7 ESXI hosts and other equipment as listed in the attachments to this ITT.

Appendix D provides a list of current equipment included in the service.

IT Support Services:

The service will provide a range of support services, including:

- Management of User Accounts
- Password management and login problem resolution
- Training for Regional Support Analysts and users
- Procurement of new equipment
- Internet Connections delivered by CRFCA
- RLI Connections (Aldershot / London only)
- Internet Security Gateway – Routine Management
- RLI Security Gateway – Routine Management
- Symphony – (First line support, linked to 2nd line support provided by SFL)
- Sharepoint

- Corporate Emails (RLI and Internet based)
- Commercial Portal (PQQ and other modules)
- AlternativeVenues.org
- Video/Tele Conference
- Virtual Desktops
- Virtual Servers
- Hardware and software upgrades, release notes, documentation changes and agreed service changes.
- CRFCA London users
- RFCAs users
- Army Cadet Force (ACF) County HQ users
- RFCA and CRFCA authorised external workers
- RFCA and CRFCA third party suppliers
- RFCA and CRFCA visitors.

A full list of user sites and user numbers to be included in the contract is provided in Appendix E.

Helpdesk support, incident logging and incident management:

The Service must include a helpdesk support service for all enquiries and incident reporting with facilities provided to allow users of the service to report incidents via three methods of communications:
- A web based customer self-service facility
- Telephone (non-premium rate number(s))
- E-mail.

All incidents, however reported, must be logged in a suitable incident and call logging system which provides escalation, progress tracking and reporting to meet the Mandatory Service Requirements (MSRs) listed in this ITT.

The MSP will pro-actively identify the root cause of incidents and take the necessary steps to prevent incidents before they occur. CRFCA management and users are to be provided with a single view of the IT Support service performance across all supported environments, including management reporting of service performance and the ability for users to track progress on individual incident tickets.

Appendix F provides statistics on the numbers of calls made to the current service over the last 12 months.

Account Management:

A Service Delivery Manager (SDM) function must be included to be responsible for the overall performance of the service and to provide a continuous point of contact to the customer for all communications regarding the service. The SDM will be the primary interface with CRFCA, and for any sub-contractors engaged in the delivery of the service. The SDM will be responsible for the overall management of the service, including:

- Monitoring and management of the ongoing provision of user services, ensuring Service Levels are met or exceeded for hardware, software deployed on the system and the network

- Ensuring that user opinion concerning the overall ABS Service and the provision of Support Services is captured and analysed
- Developing and monitoring the implementation of agreed Service Improvement Plans
- Liaising with stakeholders to ensure that service provision develops in line with evolving business needs
- Investigation of Service Level breaches, initiating action to determine any cause(s) and then implementing appropriate remedies in partnership with CRFCA
- Reporting to CRFCA on the performance of the service, through the formal reporting process. Reports will include, but not be limited to:
  - System availability
  - Operational volumes
  - Capacity Forecasts
  - Change reports
  - Security reports
  - Performance vs SLAs.

The data centre sites in the contract are:

- CRFCA Primary Data Centre, Seely House, Shoe Lane, Aldershot, Hampshire, GU11 2HJ
- CRFCA Disaster Recovery Centre, 51 Clifton Street, London, EC2A 4EY.

The above information gives an overview of the services, the equipment and the customer sites within the scope of Lot 1. Please see Appendix C for a list of the requirements for the MSP service.

Mandatory Service Requirements (MSRs), Managed Service (Lot 1)

	General:
1.	The Service must include all elements outlined in the Service Description in 4.1 above and Appendix C.
2.	Provision of support for all users across all locations as listed in the Appendices.
3.	Provision of support for all the IT and Communications equipment and software as listed, to meet the SLAs defined in Appendix G.
4.	Monitoring of all systems to ensure availability and performance in line with SLAs.
5.	Confirmation that the Supplier can meet all the defined SLAs.
6.	Management of the Data Centre and systems in Holderness House, London and Seely House, Aldershot.
7.	Standard hours of support of weekdays, 08:00 to 18:00 must be met for all services, with the addition of a technical support desk from 18:00 to 22:00 hours on weekdays and from 08:00 to 18:00 on Saturdays. All times are local UK times.
8.	Out of hours support must be available for critical issues.
9.	Provide a Single Point of Contact (SPOC) Service Desk for Incident Reporting and Incident Management.
10.	Provide an Incident logging facility via email, telephone and web.
11.	Provide 1st, 2nd and 3rd line support and manufacturers/suppliers escalation point.
12.	Provide 1st line support for 3rd party applications, including but not limited to: Symphony, Microsoft Exchange, Sharepoint, Filestore, Skype for Business and ConstructionLine.
13.	Coordination with third party hardware and software providers for 2nd and 3rd line support as required.
14.	Provide a clear escalation path for service desk calls if the response fails to meet SLAs.
15.	Provide a service portal giving access to management information on the performance of the services.
16.	Ability to provide additional ad-hoc support and project work as required throughout the term of the contract.
	Security and Quality Certification:
17.	Suppliers must have ISO27001 and ISO9001 certification or be demonstrably working towards such certification and commit to maintaining this throughout the lifetime of the contract.
18.	All processes used in the delivery of the service must be ITIL compliant.
19.	Suppliers must provide absolute compliance with JSP440 and JSP604.
20.	Location from which the services are delivered must be able to securely connect to the CRFCA Data Centre as an extension of the WAN.
21.	Location from which the services are delivered must already have or be capable of achieving Defence Assurance and Information Security (DAIS) accreditation (see https://www.gov.uk/guidance/defence-security-and-assurance-services-defence-industry-list-x). Please note that List X accreditation is not a requirement for this service.
22.	All Supplier staff engaged in the delivery of the service must be SC cleared

	prior to working on the service.
23.	The Supplier must have "Expert Partner" status with Fujitsu.
24.	The Supplier must have accredited partner status with Microsoft.
25.	The Supplier must have Authorised Reseller status for Apple products.
	Service Specific MSRs:
26.	Implementation of and adherence to an ITIL compliant Change Test and Release Management process to allow the controlled distribution and installation of authorised software applications, updates and associated data packages across the service.
27.	Use of ITIL compliant Asset Management and Configuration Management facilities to allow controlled change to the IT infrastructure and software. These changes include new releases and patches applied across the whole Service in accordance with a defined patch management plan.
28.	Maintenance and use of software to protect against virus, data loss and other threats.
29.	Maintenance of an up to date patching policy that conforms with industry standards, to minimise the vulnerability of the systems.
30.	Hardware Support including repair where possible and replacement if required of faulty equipment connected to the service.
31.	Maintenance of training materials and delivery of training to Regional Systems Administrators.
32.	Provide end user training of systems and devices, excluding Symphony.
33.	Provide end user support and advice.
34.	The Supplier shall be responsible for the management of mobile phones used by RFCAs' users using the MobileIron Mobile Device Management (MDM) system. The Supplier shall be responsible for maintaining the security and management policies for MobileIron.
35.	The Supplier shall maintain a catalogue of approved equipment that can be purchased by authorised RFCA and CRFCA users, and provide a facility through the support service SPOC for users to place orders for new equipment. Appendix H describes the current list of equipment that can be ordered through the Catalogue.
36.	The Supplier shall be responsible for all aspects of the design of the technical architecture throughout the lifetime of the contract, including hardware, software, web portals, Internet and intranet connections, firewalls, servers, and systems security.
37.	The Supplier shall be responsible for management of warranties on all equipment included within the service.

4.2　Wide Area Network Services　LOT 2

The WAN Services Provider will be responsible for the management and support of the Wide Area Network that supports the CRFCA community. The current network configuration and list of equipment is provided in Appendix J. CRFCA expects the WAN to achieve SLAs that are at least to industry standards.

Please note that firewalls are outside the scope of Lot 2.

Mandatory Service Requirements, WAN (Lot 2)

1.	The supplier must provide all WAN network service elements necessary to deliver the services.
2.	The Service must provide support for all communications and other equipment required to support the WAN, as listed in Appendix J.
3.	The Service must provide COS and QOS markings in line with industry best practice.
4.	The Service must deliver industry standard SLAs for WAN services, or better.
5.	Maintenance of all WAN hardware components to ensure achievement of availability and service levels.
6.	All processes used in the delivery of the service must be ITIL compliant.
7.	Suppliers must have ISO27001 and ISO9001 certification or be demonstrably working towards such certification and commit to maintaining this throughout the lifetime of the contract.
8.	Standard hours of support of weekdays, 08:00 to 18:00 must be met for all services, with the addition of a technical support desk from 18:00 to 22:00 hours on weekdays and from 08:00 to 18:00 on Saturdays. All times stated are UK local times.
9.	The supplier must be able to provide out of hours support as required for critical incidents.
10.	Provide an incident management facility for incidents reported to the WAN Supplier by the Managed Services Provider.
11.	Provide 1st, 2nd and 3rd line support and manufacturers/suppliers escalation point.
12.	Provide a clear escalation path for incidents if the response fails to meet SLAs.
13.	Ability to provide additional ad-hoc support and project work as required throughout the term of the contract.
14.	Hardware Support including repair where possible and replacement if required of faulty equipment connected to the service.
15.	The Supplier will be responsible for all aspects of the design of the technical architecture for the WAN throughout the lifetime of the contract.
16.	Management of warranties on all equipment must be included within the service.

5. Supplier Questionnaire

The Supplier Questionnaire (SQ) for Lot 1, the Managed Service provider, is shown in Appendix A.

The Supplier Questionnaire (SQ) for Lot 2, the WAN Service provider, is shown in Appendix B.

The relevant SQ must be completed by Tenderers and submitted along with your response to this ITT. Where a Supplier is bidding for both Lot 1 and Lot 2, a separate SQ must be provided for each Lot.

Suppliers should note the instructions in Section 6.1 below regarding the selection criteria and the evaluation of the SQ.

6. Evaluation of Responses

6.1 Overview

All completed SQ and ITT responses received will be evaluated by CRFCA. Throughout the evaluation process, the right is reserved to seek clarifications from Tenderers, where this is considered necessary to achieve a full understanding of the proposals received.

The evaluation will be conducted in two stages as described in Sections 6.2 and 6.3 below. The objective of the first stage will be to assess the Tenderer's Supplier Questionnaire (SQ) and responses to Part A of the ITT against selection criteria which will confirm Tenderers suitability as a potential service provider. Suppliers who do not submit a satisfactory response to the SQ will not be considered for further evaluation.

For those Tenders which pass the first stage of the evaluations, the second stage of the evaluation will assess the most economically advantageous tender. This will be carried out by an evaluation of the Tenderer's qualitative responses to Part B of the ITT, plus your Tendered price, as described in the evaluation and award criteria outlined below.

The same evaluation approach, as outlined above, will be applied to each of the two Lots covered by this ITT.

6.2 Stage 1 – Selection Criteria

Selection criteria are designed to check that potential service providers meet or exceed the minimum expectations and requirements of CRFCA. Where selection criteria are of a 'pass/fail' nature and if a Tenderer fails against any one or more of these selection criteria, then grounds will exist to exclude that ITT response from any further consideration.

Compliance with the minimum standards will be checked by reference to the information given by Tenderers in the questionnaire section of the ITT response document. The minimum standards themselves are summarised in the table set out below.

Please be mindful when completing your ITT response that if your answer is unsatisfactory in regard to any of the areas detailed in the table below, your response will be rejected.

Section		Selection Criteria
1	**Completion of Supplier Questionnaire**	The Supplier Questionnaire (SQ) must be fully completed in the format provided in Appendix A for Lot 1, or Appendix B for Lot 2.
		Any SQ that does not meet the required levels of suitability will be excluded and ITTs from that supplier will not be assessed. Tenderers should note that where a requirement is listed in the SQ as being mandatory, a failure to meet this requirement will result in the Tenderer being excluded and the ITT from that Tenderer not being assessed.

Section		Selection Criteria
2	**Financial Stability**	Financial stability will be assessed. To permit this to assessment, Tenderers are required to provide their latest three years audited financial statements for CRFCA to evaluate.
3	**Insurance**	For insurance cover, the requirement is for a minimum of £5 million for public liability, £5 million employer's liability and £5 million professional indemnity. Tenderers that do not currently hold these levels of insurance must satisfy CRFCA that they will hold these levels of cover for any contract awarded to their organisation, at no extra cost to CRFCA. Any Tenderer who does not have these levels of insurance and will not agree to increase insurance to these levels will fail.
4	**Mandatory Service Requirements**	The Tenderer's response must meet all Mandatory Service Requirements (MSRs), including all Security and Quality standards.

6.3   Stage 2 – Award Criteria

For the avoidance of doubt, only those Tenderers that pass the Selection Criteria will proceed to have their tender submissions evaluated against the Award Criteria.

CRFCA will take into account the quality of the tender as well as the tendered prices and rates, (quality 60% and price 40%), fitness for purpose and any other factors relevant to the services, its supply and any other requirements of the services.

CRFCA reserves the right not to award the contract to the lowest or any Tenderer, reserving also the right to accept the same in whole or in part.

Any acceptance of a tender by CRFCA shall be in writing and shall be communicated to the Tenderer following a standstill period (from the date of the notification of proposal to award is sent to all Tenderers) of not less than 10 days. Upon acceptance the contract shall thereby be constituted and become binding on both parties notwithstanding which the Tenderer shall, upon request of CRFCA, forthwith execute a formal contract.

The award criteria process outlined above will apply to each of the Lots covered by this ITT.

6.4   Qualitative Evaluation

For each Lot within this ITT, the qualitative evaluation is worth a total of 60% of the overall score.

Tenderers are invited to submit a qualitative submission against each of the questions set out in either Section 7 of this ITT (for Lot1, Managed Service Provider), and / or Section 8 of the ITT for Lot 2, WAN Services.

CRFCA will assess Tenderers responses to each heading against the criteria set out in the tables below and will award points up to the maximum shown against each heading. The maximum total points available for each section are as shown in the following tables.

Lot 1 – Managed Service Provider:

Category	Component	Maximum Score per Component	Weighting	Points Available
General Response Requirement Response Part A No score is attached.				
Question 1	Company contact details	N/A	N/A	N/A
Question 2	Quality Certifications	Pass/fail	Pass/fail	N/A
Question 3	Business Activities	Pass/fail	Pass/fail	N/A
Question 4	Company Policies	Pass/fail	Pass/fail	N/A
Response Requirement Response Part B Scored as detailed below.				
Question 5 (1 Part)	Solution Summary	5	20	100
Question 6 (1 part)	Mandatory Service Requirements	Pass/fail	Pass/fail	N/A
Question 7 (8 parts)	Contracts and Commercial Approach	Pass/fail	Pass/fail	N/A
Question 8 (71 parts)	Operational Information (Parts 1 and 2)	5	1	355
Question 9 (17 parts)	Account Management	5	1	85
Question 10 (25 parts)	Third Party Product Support	5	1	125
Question 11 (5 parts)	Security	5	4	100
Question 12 (10 parts)	Disaster Recovery	5	2	100

Question 13 (7 parts)	Transition	5	3	105
Question 14 (5 parts)	Implementation Planning	5	4	100
Question 15 (5 parts)	Exit Planning	5	2	50
Question 16 (1 part)	Executive Summary	5	10	50
Total	**Total Points available:**			**1170**

Lot 2 – WAN Service Provider:

Category	Component	Maximum Score per Component	Weighting	Points Available
General Response Requirement No score is attached.	**Response Part A**			
Question 1	Company contact details	N/A	N/A	N/A
Question 2	Quality Certifications	Pass/fail	Pass/fail	N/A
Question 3	Business Activities	Pass/fail	Pass/fail	N/A
Question 4	Company Policies	Pass/fail	Pass/fail	N/A
Response Requirement Scored as detailed below.	**Response Part B**			
Question 5 (1 Part)	Solution Summary	5	15	75
Question 6 (1 Part)	Mandatory Service Requirements	Pass/fail	Pass/fail	N/A
Question 7 (12 parts)	Contracts and Commercial Approach	Pass/fail	Pass/fail	N/A
Question 8 (38 parts)	Operational Information (part 1)	5	1	190
Question 9 (30 parts)	Operational Information (part 2)	5	1	150
Question 10 (7 parts)	Background Information	5	1	35
Question 11 (7 parts)	Security	5	2	70
Question 12 (10 parts)	Disaster Recovery	5	1	50
Question 13 (12 parts)	Account Management and Service Reporting	5	1	60
Question 14 (6 parts)	Transition	5	1	30
Question 15 (5 parts)	Implementation Planning	5	2	50
Question 16 (6 parts)	Exit Planning	5	1	30
Question 17 (1 part)	Executive Summary	5	10	50
Total	**Total Points available:**			**790**

6.5   Scoring Methodology

Scores will be given for the response to each Question according to the following criteria. Where an answer is either "Yes" or "No" (with no further qualification), the score will be either 5 or 0.

Assessment	Score
No response provided / Extremely unsatisfactory response: No answer is provided, or the answer completely fails to demonstrate that any of the CRFCA requirements in the area being measured will be delivered.	Score 0 points
Highly unsatisfactory response: Provides only very limited assurance that the CRFCA requirements in the area being measured will be delivered.	Score 1 point
Unsatisfactory response: Demonstrates how some of the CRFCA requirements in the area being measured will be delivered so as to provide a basic service that will be reasonably responsive to the needs of CRFCA and other stakeholders.	Score 2 points
Satisfactory response: Demonstrates how most of the CRFCA requirements in the area being measured will be delivered so as to provide an acceptable service that will mostly be responsive to the needs of CRFCA and other stakeholders.	Score 3 points
Highly satisfactory response: Demonstrates how all of the CRFCA requirements in the area being measured will be delivered so as to provide a good service that will be responsive to the needs of CRFCA and other stakeholders.	Score 4 points
Excellent response: Demonstrates clearly how all of the CRFCA requirements in the area being measured will be fully delivered so as to deliver an excellent service that will be highly responsive to the needs of CRFCA and other stakeholders.	Score 5 points

Failure to score a minimum of three (3) in any one category may result in the ITT response being disqualified.

6.6   Financial Evaluation

The Tenderer who submits the overall lowest priced bid will receive the full weighting available for the financial evaluation, which is 40%.

The other Tenderers will be scored as against the overall lowest priced bid, in the manner described below:

A score of 40 will be allocated to the lowest price; the price on the remaining tenders will be calculated using a percentage (%) difference method, as follows:

Pricing Score = Total Available Marks x (Lowest Priced Technically and Commercially Compliant Tender) / Tender Price

Example:
Tenderers total price = 125
Lowest Compliant price = 100
Tenderers score = 40 x 100/125 = 32 points

CRFCA have identified the risk that abnormally low bids and abnormally high bids may be received. If this risk is not correctly managed, it has the potential to distort the evaluation process. To manage this risk, CRFCA will evaluate each response from a commercial perspective and if, in the reasonable opinion of the CRFCA commercial team, it is considered that a bid falls into one of these categories, the Tenderer will be asked to clarify and explain in writing the price or cost of their bid (in accordance with the Public Contracts Regulations 2015). CRFCA shall assess the information provided by the Tenderer and may reject the tender where the evidence supplied does not satisfactorily account for the level of price or costs proposed by the Tenderer.

CRFCA reserves the right not to award the contract to the lowest or any Tenderer, reserving also the right to accept the same in whole or in part.

7. Managed Services Provider (LOT 1) – Responses Required

Tenderers for LOT 1 must provide a completed Supplier Questionnaire (SQ – see Appendix A) along with responses to Part A and Part B of this ITT, below, <u>using the Microsoft Excel template in Appendix L</u>. For the avoidance of doubt, Tenderers must respond to all the questions within this section. In the case of a Tenderer who is submitting Tenders for both LOT 1 and LOT 2, a completed SQ, along with a response to the appropriate sections of this ITT must be submitted for each Lot.

General Response Requirement   Response Part A; Company Information

1.	**Contact Points for Response**	
ID	**Question**	**Answer**
1.1.	Name of the organisation in whose name the response will be submitted.	
1.2.	Contact name for enquiries about this bid.	
1.3.	Contact position (job title).	
1.4.	Address & Post Code of organisation.	
1.5.	Telephone number(s).	
1.6.	Email address.	

2.	**Quality Certifications**	
ID	**Question**	**Answer**
2.1.	Please provide your company's Data Protection registration number.	
2.2.	Does your organisation hold a UKAS recognised quality management certification?	Yes / No
2.3.	If your organisation does not hold UKAS recognised quality management certification, does your organisation have a quality management system?	Yes / No
2.4.	Is your Quality Management System conformant with ITIL?	Yes / No
2.5.	Does your organisation hold a UKAS recognised ISO 14001 certification?	Yes / No
2.6.	Does your organisation hold a UKAS recognised ISO 27001 certification?	Yes / No
2.7.	Please provide a summary of any other certifications your organisation holds that you consider are relevant to this opportunity.	

3.	**Business Activities**	
ID	**Question**	**Answer**
3.1.	Provide a brief summary of what are the main business activities of your organisation? (Maximum 250 words).	
3.2.	How many full time wholly employed staff does your organisation have in total?	

ID	Question	Answer
3.3.	How many technical / support staff with the capability to deliver these services does your organisation have?	
3.4.	How many administrative support staff does your organisation have?	

4.	Policies	
ID	**Question**	**Answer**
4.1.	Does your organisation have a written Health and Safety at work policy? If 'No', please explain why and what your arrangements are regarding Health and Safety.	Yes / No
4.2.	Does your organisation have a health and safety at work system? If 'No', please explain why and what your arrangements are regarding Health and Safety.	Yes / No
4.3.	Has your company ever been prosecuted for a breach of Health & Safety legislation? If "Yes" to the above, then please provide more information about the breach(es).	Yes / No
4.4.	Has your organisation formally documented its approach and/or policies in regard to Corporate Social Responsibility?	Yes / No
4.5.	Does your organisation have a written equal opportunities policy?	Yes / No
4.6.	Does your organisation have a written environmental policy?	Yes / No
4.7.	Does your organisation have a written policy on anti-bribery and anti-corruption measures?	Yes / No
4.8.	Does your organisation have a written policy regarding modern slavery?	Yes / No
4.9.	Does your organisation have a formal, documented, Data Protection policy?	Yes / No
4.10.	Does your organisation have a formal, documented, Data Security policy?	Yes / No
4.11.	Is your organisation currently compliant with General Data Protection Regulation (GDPR)?	Yes / No
4.12.	Does your organisation have a formal, documented, ICT Security policy?	Yes / No
4.13.	Does your organisation have formal, documented, Business Continuity and Disaster Recovery policies?	Yes / No
4.14.	Does your organisation publish gender pay gap information? If yes, please provide details.	Yes / No Plus details, if "Yes"
4.15.	Does your organisation work with any organisations that have ever been convicted of a criminal offence related to: Childhood exploitation, Human rights violation, Legislation on equal pay, Environmental	Yes / No Plus details, if "Yes"

	exploitation, Breach of employment rights? If Yes, please provide details.	
4.16.	Please provide PDF copies of any policies or information referenced within this section.	

Response Requirement   Response Part B; Proposed Service Approach

5.		Solution Summary	
ID		**Question**	**Answer**
5.1.		Provide a summary of the operational and technical solution that you propose to meet this requirement. (The response to this question must be no longer than 2000 words).	Description

6.		Mandatory Service Requirements	
ID		**Question**	**Answer**
6.1.		Does the solution you propose deploying fully comply with each of the Mandatory Service Requirements listed in Section 4.1 of this ITT? **Tenderers should note that further evaluation will not be undertaken for any response which does not provide compliance with the Mandatory Service Requirements.**	Yes / No

7.		Contractual and Commercial Considerations	
ID		Question	**Answer**
7.1.		CRFCA intend to establish a contract for an initial period of 5 years with an option to extend for an additional 2 years. Please confirm your acceptance with this requirement, or an explanation if not.	Yes / No Plus explanation if required
7.2.		Confirm that you have provided a copy of the terms and conditions that you propose for this engagement. These should be provided as a separate document.	Yes / No
7.3.		Confirm that, where the solution provided includes software, your terms and conditions must include a provision that you have full rights to all the software to be provided to CRFCA under the contract and that CRFCA will be indemnified against any third-party claims for intellectual property rights where these have been bundled or re-sold by you.	Yes / No
7.4.		Are you willing to participate in annual contract and consultancy rate benchmarking?	Yes / No
7.5.		Are you prepared to agree to joint benchmarking funding, capped at a maximum cost to you of £10,000 per annum, should this option be exercised?	Yes / No

7.6.	Any contract which includes a term which would bind CRFCA for longer than 12 months must also contain a term which provides for cancellation of the agreement in the event that by that time, the solution provided has been found to be unfit for purpose. Please confirm your acceptance to this clause.	Yes / No
7.7.	Will this project / contract be wholly delivered by your organisation, or will partners, subcontractors, or associates be utilised? If third parties will be involved, please list them and state their role in the delivery of the service.	
7.8.	How many UK customers does your company deliver comparable services to?	

8.	Operational Information	
ID	**Question**	**Answer**
	Overview of Solution Elements:	
8.1.	Please describe how you will meet the requirement for Software Development services, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.2.	Please describe how you will meet the requirement for a PH2 Catalogue Service, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.3.	Please describe how you will meet the requirement for Professional Services, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.4.	Please describe how you will meet the requirement for Telecomm Services, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.5.	Please describe how you will meet the requirement for Third Party Supplier Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.6.	Describe how you ensure that interfaces with other suppliers are managed effectively, ensuring that the service provided to CRFCA is optimised?	
8.7.	Please describe how you will meet the requirement for Software Licensing Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.8.	Please describe how you will meet the requirement for Site Coordinating Installation Design Authority SCIDA Liaison, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.9.	Please describe how you will meet the requirement for Change Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	

8.10.	Please describe how you will meet the requirement for RFCA / ACF On-Site Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.11.	Please describe how you will meet the requirement for R&D, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.12.	Please describe how you will meet the requirement for Secure WiFi Services, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.13.	Please describe how you will meet the requirement for Security Management Services, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.14.	Please describe how you will meet the requirement for Asset Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.15.	Please describe how you will meet the requirement for a Helpdesk Service, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.16.	Please describe how you will meet the requirement for SLA Management and Reporting, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.17.	Please describe how you will meet the requirement for User Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.18.	Please describe how you will meet the requirement for Log Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.19.	Please describe how you will meet the requirement for Network Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.20.	Please describe how you will meet the requirement for Data Centre Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.21.	Please describe how you will meet the requirement for Business Continuity Planning (BCP) Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.22.	Please describe how you will meet the requirement for Mobile Device Management (MDM), as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.23.	Please describe how you will meet the requirement for Configuration Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.24.	Please describe how you will meet the requirement	

	for Internal Audit Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.25.	Please describe how you will meet the requirement for support for Freedom of Information (FOI) requests, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.26.	Please describe how you will meet the requirement for GDPR compliance, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.27.	Please describe how you will meet the requirement for Third Party Applications Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.28.	Please describe how you will meet the requirement for Client Applications Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.29.	Please describe how you will meet the requirement for Level 1, Level2 and Level 3 Systems Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.30.	Please describe how you will meet the requirement for DNS Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.31.	Please describe how you will meet the requirement for Level 4 Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.32.	Please describe how you will meet the requirement for remote User Support, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.33.	Please describe how you will meet the requirement for Appliances, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.34.	Please describe how you will meet the requirement for Server Management Services, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.35.	Please describe how you will meet the requirement for Internet DNS Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.36.	Please describe how you will meet the requirement to support Systems Applications, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.37.	Please describe how you will meet the requirement for Active Directory Management, as outlined in the Service Catalogue spreadsheet included in Appendix C.	
8.38.	Describe your approach to Installations, Moves,	

	Additions and Changes (IMACS) and the charging methods that are applied to IMACS by your organisation.	
8.39.	CRFCA will require that an SLA for firewall changes is established. Tenderers should describe their typical approach to this area, providing a proposed SLA that can be reviewed by CRFCA, which will include SLA detail, classifications and priorities. We would like to understand the proposed approach to emergency, high priority and scheduled firewall changes, together with the attaching timescales.	
8.40.	Describe how you would deliver training to defined "Regional Systems Administrators" within the user base for the service?	
8.41.	Describe how you would deliver end user training	
8.42.	Please list the core technical competencies of your organisation. Include detail of what you consider to be the key technology areas supported by the business. (Maximum 500 words).	
8.43.	What technical and quality certifications does your organisation hold?	
8.44.	Please confirm the number of installation and support engineering staff your organisation employs.	
8.45.	How would on-site engineering support be provided to CRFCA sites in Seeley House, Aldershot and Holderness House, London. Does your organisation have engineering resources located in or near these areas?	
8.46.	How would on-site engineering support be provided to CRFCA sites listed in Appendix E, including sites that are remote from your own offices? Does your organisation have engineering resources located in or near these areas?	
8.47.	How will you provide hardware support, including equipment replacement if required, across the sites in the scope of the contract?	
8.48.	Do you provide a Service Desk and support services? If yes, at what level(s) i.e. 1st, 2nd or 3rd.	
8.49.	Are all Service Desk support services within the support hours delivered by internal resource?	
8.50.	Are all out of hours Service Desk support services delivered by internal resource?	
8.51.	Do you have experience of providing support services using security cleared personnel?	
8.52.	Provide a high level summary of your standard Support and Maintenance process (500 words)	

8.53.	Do you operate a manned 24 x 7 x 52 support operation? If not, please describe how you provide such support if required.	
8.54.	If not what are your standard service hours?	
8.55.	What is your definition of a standard business day for Service Desk support?	
8.56.	What methods can clients use to raise Incidents with your Service Desk?	
8.57.	What methods does your Service Desk use to provide clients with alerts?	
8.58.	How does your response to a monitor alert differ from the response to a customer raised incident?	
8.59.	How does the support operation differ, if at all, at different times of the day/night?	
8.60.	How does the support operation differ, if at all, at weekends?	
8.61.	How does the support operation differ, if at all, on public holidays?	
8.62.	How do you ensure you over achieve against SLA targets?	
8.63.	How do you measure your performance against SLA targets?	
8.64.	Provide an example monthly service performance report.	
8.65.	Provide a summary of the process you use to record, manage and report Incidents.	
8.66.	Provide detail of the knowledge base(s) that will be used by your operation to support the service.	
8.67.	Describe the nature and capability of your first line support teams.	
8.68.	Describe the nature and capability of your second line support teams.	
8.69.	Describe the nature and capability of your third line support teams.	
8.70.	How does your support operation monitor systems and installed network connections?	
8.71.	Provide detail of your Incident escalation process.	

9.	**Account Management Information**	
ID	**Question**	**Answer**
9.1.	Provide a brief summary describing how you will monitor the performance of your proposed services. (Maximum 500 words).	
9.2.	Describe your standard Account Management process and who our nominated Account Manager would be should we proceed?	
9.3.	How many accounts would our Account Manager be responsible for?	
9.4.	Based on the anticipated spend, where would the CRFCA contract reside within the Account	

ID	Question	Answer
	Mangers portfolio? Top quartile, if not top quartile, then where?	
9.5.	How many of the customers receive a managed service from your organisation, similar to CRFCA's requirements?	
9.6.	Based on your proposed solution(s), where would the annual contract value of the CRFCA contract sit in your client base, i.e. Position 34.	
9.7.	Based on your proposed solution(s), where would the total contract value of the CRFCA contract sit in your client base, i.e. Position 26.	
9.8.	How do you develop and maintain customer relationships?	
9.9.	Describe any initiatives that you are, or have recently, undertaken that deliver innovation to your customers.	
9.10.	How do you respond to customer dissatisfaction or failures to meet SLA targets?	
9.11.	How do you ensure that an account team does not have an excessive churn of staff?	
9.12.	There should be a named individual responsible for delivery of this service and a succession plan established, in case the individual is unavailable. Describe how this requirement be delivered.	
9.13.	There should be a contingency plan in place for key members of the proposed project delivery team. Describe how this requirement will be delivered.	
9.14.	Please outline your standard reporting following an SLA failure, including report KPIs and root cause analysis.	
9.15.	How would you manage change control to the contract and / or services?	
9.16.	Describe your approach to Continuous Improvement and how it would be implemented against the CRFCA contract.	
9.17.	What are the likely or potential areas of improvement you would expect to make to the services in the first 2 years or running the service?	

10.	**Third Party Product Support Requirements**	
ID	**Question**	**Answer**
10.1.	What Microsoft software products do you provide or support?	
10.2.	What Microsoft software accreditations do you hold?	
10.3.	What is your Microsoft partnership status?	
10.4.	What experience do you have in supporting Microsoft products?	

10.5.	What Fujitsu products do you provide or support?	
10.6.	What Fujitsu accreditations do you hold?	
10.7.	What is your Fujitsu partnership status?	
10.8.	What experience do you have in supporting Fujitsu hardware?	
10.9.	What Apple products do you provide or support?	
10.10.	What Apple accreditations do you hold?	
10.11.	What is your Apple partnership status?	
10.12.	What experience do you have in supporting Apple hardware?	
10.13.	What software accreditations, other than Microsoft, do you hold?	
10.14.	What partnerships do you have with software and hardware manufacturers or vendors, other than Microsoft, Fujitsu and Apple?	
10.15.	What hardware products do you provide or support other than Fujitsu and Apple?	
10.16.	What hardware accreditations do you hold other than Fujitsu and Apple?	
10.17.	What is your level of experience in supporting each of the following products (1000 words): • Veeam • Brocade • Sharepoint • Microsoft Exchange • McAfee Anti-Virus • ConstructionLine application • Symphony financial software • MobileIron MDM • VMWare • Citrix • Cisco	
10.18.	What experience do you have in supporting the Avaya VOIP platform?	
10.19.	What experience do you have in supporting the MobileIron MDM platform?	
10.20.	What accreditations or certifications do you have for service desk, service delivery, security or related processes?	
10.21.	Describe your relevant staff team structures, highlighting relevant skills and certifications by each role. Please include organisation charts, if necessary as separate documents, where appropriate.	
10.22.	Describe the Datacentres that are used by your company and their locations.	
10.23.	Which virtualisation technologies does your organisation support?	
10.24.	Detail any virtualisation certifications held by	

	your organisation.	
10.25.	How many of your full-time employees hold certifications in relation to virtualisation technologies? List number and technologies.	

11.	Security	
ID	**Question**	**Answer**
11.1.	How do you propose to secure the CRFCA environment to meet the requirements and standards outlined in this ITT?	
11.2.	How will intrusion be detected and prevented?	
11.3.	What will happen in the event of an unauthorised access to the network and to our systems?	
11.4.	If the above occurs, how are the identified risks minimised?	
11.5.	Confirm that the design of the Services will be undertaken in absolute compliance with Industry Standards, best practice and that the design will be fully documented and shared with CRFCA.	

12.	Disaster Recovery	
ID	**Question**	**Answer**
12.1.	Describe your organisation's levels of infrastructure, staff and locations resilience ensuring at all times a continuous service to your clients?	
12.2.	Describe your organisation's approach to Disaster Recovery (DR) for incidents that affect your own organisation, or supply chain.	
12.3.	Describe your organisation's approach to Business Continuity Planning (BCP) for incidents that affect your own organisation, or supply chain.	
12.4.	How would you propose to provide a robust approach to the support of the CRFCA infrastructure, in the event of a disaster impacting their business?	
12.5.	Detail how you would manage and prioritise multiple client DR invocations, such as in the event of a large-scale infrastructure failure impacting adversely upon the operation of your organisation.	
12.6.	How are increases and/or changes to the primary customer environment and DR environment managed from a commercial perspective?	
12.7.	What is the level and frequency of DR and BCP testing that your organisation carriers out?	
12.8.	Are the above tests independently ratified by external third parties?	

ID	Question	Answer
12.9.	Provide a copy of your current DR/BCP Plan.	
12.10.	Provide a copy of your most recent test results.	

13.	**Transition**	
ID	**Question**	**Answer**
13.1.	Provide an overview of your plan and approach to the transition of the service. (The response to this question must be no longer than 1000 words).	
13.2.	Provide a forecast of the transition timescale that you would typically expect for a service of this nature.	
13.3.	What notice period would your company require before a service transition could commence?	
13.4.	Would you commit to contractual delivery dates for the provision of the required services?	
13.5.	What penalties would you propose for failure to meet these delivery dates?	
13.6.	How would you ensure any such failures do not financially impact CRFCA in any way?	
13.7.	What is your experience of transitioning a service into your company in the case of TUPE? Your attention is drawn to the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE), as amended. CRFCA would be neither transferor nor transferee of the employees in the circumstances of any contract awarded as a result of this invitation and it is your responsibility to consider whether or not TUPE applies to this re-let and to tender accordingly. Notwithstanding this, you will wish to note that it is CRFCA's view that TUPE is likely to be applicable if this Invitation to Tender results in a Contract being placed, although CRFCA shall not be liable for the opinion expressed above. In these circumstances CRFCA will wish to satisfy itself that your proposals are responsibly based and take full account of your likely TUPE obligations.	

14.	**Implementation Planning**	
ID	**Question**	**Answer**
14.1.	Provide details of the implementation transition planning undertaken for an engagement of this nature.	
14.2.	Tenderers should describe how they would work with the current CRFCA Supplier(s) to ensure the	

	successful delivery of the implementation.	
14.3.	Tenderers should describe their approach to the management of risk and provide an initial risk register relating to this project.	
14.4.	Provide details of key tasks and their ownership required for implementation planning.	
14.5.	Provide an implementation plan detailing the typical implementation of an engagement of this nature. The implementation plan should contain a Gantt chart that provides detail of the proposed approach and timescales. (The response to this question must be no longer than 1000 words).	

15.	**Exit Planning**	
ID	**Question**	**Answer**
15.1.	Provide details of the exit planning which would be undertaken for an engagement of this nature.	
15.2.	Provide details of key tasks and their ownership required for exit planning.	
15.3.	At the end of the contract period, if there are any sub-contracted services in place, can these all if necessary be novated to an alternative supplier?	
15.4.	Detail all exit charges that might be incurred by CRFCA at the end of the agreed contractual term if we were to change supplier.	
15.5.	At the end of the contract period, is it possible for 90-day rolling extension periods to be put in place, if requested by CRFCA? If yes, what would be the commercial calculation for this extension?	

16.	**Executive Summary**	
ID	**Question**	**Answer**
16.1.	Please provide an executive summary of your proposal. (The response to this question must be no longer than 1000 words).	

Financial Response Requirement   Financial Evaluation

Financial Evaluation	Provide a description of your proposed commercial model and costs for delivering these services using the template spreadsheet provided in Appendix I.	

8. Wide Area Network, LOT 2 - Responses Required

Tenderers for LOT 2 must provide a completed Supplier Questionnaire (SQ) using the format prescribed in Appendix B along with responses to Part A and Part B of this ITT, below, using the Microsoft Excel template in Appendix M. For the avoidance of doubt, Tenderers must respond to all the questions within this section. In the case of a Tenderer who is submitting Tenders for both LOT 1 and LOT 2, a completed SQ, along with a response to the appropriate sections of this ITT must be submitted for each Lot.

General Response Requirement   Response Part A; Company Information

1.	Contact Points for Response	
ID	**Question**	**Answer**
1.1	Name of the organisation in whose name the response will be submitted.	
1.2	Contact name for enquiries about this bid.	
1.3	Contact position (job title).	
1.4	Address & Post Code of organisation.	
1.5	Telephone number(s).	
1.6	Email address.	

2.	Quality Certifications	
ID	**Question**	**Answer**
2.1	Please provide your company's Data Protection registration number.	
2.2	Does your organisation hold a UKAS recognised quality management certification?	Yes / No
2.3	If your organisation does not hold UKAS recognised quality management certification, does your organisation have a quality management system?	Yes / No
2.4	Is your Quality Management System conformant with ITIL?	Yes / No
2.5	Does your organisation hold a UKAS recognised ISO 14001 certification?	Yes / No
2.6	Does your organisation hold a UKAS recognised ISO 27001 certification?	Yes / No
2.7	Please provide a summary of any other certifications your organisation holds that you consider are relevant to this opportunity.	

3.	Business Activities	
ID	**Question**	**Answer**
3.1	Provide a brief summary of what are the main business activities of your organisation? (Maximum 250 words).	

3.2	How many full time wholly employed staff does your organisation have in total?	
3.3	How many technical / support staff with the capability to deliver these services does your organisation have?	
3.4	How many administrative support staff does your organisation have?	

4.	**Policies**	
ID	**Question**	**Answer**
4.1	Does your organisation have a written Health and Safety at work policy? If 'No', please explain why and what your arrangements are regarding Health and Safety.	Yes / No
4.2	Does your organisation have a health and safety at work system? If 'No', please explain why and what your arrangements are regarding Health and Safety.	Yes / No
4.3	Has your company ever been prosecuted for a breach of Health & Safety legislation? If "Yes" to the above, then please provide more information about the breach(es)	Yes / No
4.4	Has your organisation formally documented its approach and/or policies in regard to Corporate Social Responsibility?	Yes / No
4.5	Does your organisation have a written equal opportunities policy?	Yes / No
4.6	Does your organisation have a written environmental policy?	Yes / No
4.7	Does your organisation have a written policy on anti-bribery and anti-corruption measures?	Yes / No
4.8	Does your organisation have a written policy regarding modern slavery?	Yes / No
4.9	Does your organisation have a formal, documented, Data Protection policy?	Yes / No
4.10	Does your organisation have a formal, documented, Data Security policy?	Yes / No
4.11	Is your organisation currently compliant with General Data Protection Regulation (GDPR)?	Yes / No
4.12	Does your organisation have a formal, documented, ICT Security policy?	Yes / No
4.13	Does your organisation have formal, documented, Business Continuity and Disaster Recovery policies?	Yes / No
4.14	Does your organisation publish gender pay gap information? If yes, please provide details.	Yes / No Plus details, if "Yes"
4.15	Does your organisation work with any organisations that have ever been convicted of a criminal offence related to:	Yes / No Plus details, if "Yes"

	Childhood exploitation, Human rights violation, Legislation on equal pay, Environmental exploitation, Breach of employment rights? If Yes, please provide details.	
4.16	Please provide PDF copies of any policies or information referenced within this section.	

Response Requirement   Response Part B; Proposed Service Approach

5.	Solution Summary	
ID	**Question**	**Answer**
5.1.	Provide a summary of the solution that you propose to meet the WAN Services requirement. (The response to this question must be no longer than 1000 words).	Description

6.	Mandatory Service Requirements	
ID	**Question**	**Answer**
6.1.	Does the solution you propose deploying fully comply with each of the Mandatory Service Requirements listed in Section 4.2 of this ITT? **Further evaluation will not be undertaken for any response which does not provide compliance with the Mandatory Service Requirements.**	Yes/No Description

7.	Contractual & Commercial Considerations	
ID	**Question**	**Answer**
7.1.	What contractual term(s) and duration would you propose for a service of this nature?	
7.2.	Confirm that you have provided a copy of the terms and conditions that you propose for this engagement. These may be provided as a separate document.	Yes/No
7.3.	Confirm that, where the solution provided includes software, your terms and conditions must include a provision that you have full rights to all the software to be provided to CRFCA under the contract and that CRFCA will be indemnified against any third-party claims for intellectual property rights where these have been bundled or re-sold by you.	Yes/No
7.4.	Are you willing to participate in annual contract and consultancy rate benchmarking?	Yes / No
7.5.	Are you prepared to agree to joint benchmarking funding, capped at a maximum cost to you of £10,000 per annum, should this option be exercised?	Yes / No
7.6.	Any contract which includes a term which would	Yes / No

	bind CRFCA for longer than 12 months must also contain a term which provides for cancellation of the agreement in the event that by that time, the solution provided has been found to be unfit for purpose. Please confirm your agreement to this clause.	
7.7.	Will this project / contract be wholly delivered by your organisation, or will carriers, partners, subcontractors, or associates be utilised? If third parties will be involved, please list them and state their role in the delivery of the service.	Yes / No Plus description if "No"
7.8.	How many UK customers has your company delivered comparable services to?	
7.9.	Provide details of your proposed SLAs for the CRFCA WAN and your standard SLAs for WAN services, along with an explanation for any differences between the two.	
7.10.	How do you ensure you over achieve against SLA targets?	
7.11.	How do you measure your performance against SLA targets?	
7.12.	What penalties are there should you fail to meet these SLAs?	

8.	**Operational Information, part 1**	
ID	**Question**	**Answer**
8.1.	Please list the core technical competencies of your organisation. (Maximum 250 words).	
8.2.	What technical certifications does your organisation hold?	
8.3.	Please confirm the number of installation/support engineering staff your organisation employs.	
8.4.	Describe how you would ensure a high level of service availability and resilience for the WAN, including achievement of the SLAs outlined in your response to 7.9 above.	
8.5.	Can you deliver and install appropriate copper infrastructure cabling?	Yes / No
8.6.	Can you deliver and install appropriate fibre optic cabling infrastructure?	Yes / No
8.7.	What other, additional, services does your organisation have capability to deliver?	
8.8.	Do you provide a Service Desk and support service to allow for reporting of incidents relating to the WAN? If Yes, please describe.	Yes / No Plus description if "Yes"
8.9.	Are all support services delivered by internal resource?	Yes / No
8.10.	Are all out of hours support services delivered by	Yes / No

	internal resource?	
8.11.	Provide a high level summary of your standard Support and Maintenance process.	
8.12.	Do you operate a manned 24 x 7 x 52 support operation?	Yes / No
8.13.	What are your standard days/hours coverage/support of support? (e.g.: 24 x 7 x 52).	
8.14.	What methods can clients use to raise Incidents relating to the WAN?	
8.15.	What methods do you use to provide clients with alerts?	
8.16.	How does your response to a monitor alert differ from the response to a customer raised incident?	
8.17.	How does the support operation differ, if at all, at different times of the day/night?	
8.18.	How does the support operation differ, if at all, at weekends?	
8.19.	How does the support operation differ, if at all, on public holidays?	
8.20.	Provide a summary of the response times that you are able to provide.	
8.21.	Provide a summary of the target resolution times that you are able to provide.	
8.22.	Provide detail of the communication mechanisms that you use to interface with clients.	
8.23.	Provide a summary of the process you use to record, manage and report Incidents.	
8.24.	Provide detail of the knowledge base(s) used by your operation.	
8.25.	Describe the nature and capability of your first line support teams.	
8.26.	Describe the nature and capability of your second line support teams.	
8.27.	Describe the nature and capability of your third line support teams.	
8.28.	How does your support operation monitor systems and installed network connections?	
8.29.	Provide detail of your Incident escalation process.	
8.30.	Describe how you ensure that interfaces with other suppliers are managed effectively, ensuring that the service provided to CRFCA is optimised?	
8.31.	How and where will you deliver Internet services to the CRFCA WAN?	
8.32.	Which carrier will provide Internet transit?	
8.33.	How resilient is the Internet transit?	
8.34.	CRFCA require the end devices (routers) to be managed by the supplier. Please confirm this is the case for your proposed solution.	Yes / No
8.35.	Please describe the make and model of the end devices (routers) that will be used at CRFCA	

	locations to deliver your proposed solution.	
8.36.	Confirm that all end devices (routers) have software subscription and management included within the costs provided.	Yes / No
8.37.	Please explain how the end devices (routers) will be managed at contract cessation.	
8.38.	Describe your approach to Installations, Moves, Additions and Changes (IMACS) and the detailed charging methods that are applied to IMACS by your organisation. (500 words)	

9.	Operational Information, part 2	
ID	**Question**	**Answer**
9.1.	How many VM WANs has your company delivered over the last 12 months?	
9.2.	What was the average order to delivery time for VM WANs over the last 12 months?	
9.3.	What was the average delivery lead time for VM WANs over the last 12 months?	
9.4.	What was the most delayed delivery time for a VM WAN over the last 36 months?	
9.5.	What is the availability SLA for VM WANs?	
9.6.	Is 100% resilience guaranteed, at every point, for VM WANs?	Yes / No
9.7.	What WAN and end point management is included within VM WANs?	
9.8.	How many VM WANs have your provision within the last 36 months?	
9.9.	What is your approximate annual spend with VM?	
9.10.	How many BT WANs has your company delivered over the last 12 months?	
9.11.	What was the average order to delivery time for BT WANs over the last 12 months?	
9.12.	What was the average delivery lead time for BT WANs over the last 12 months?	
9.13.	What was the most delayed delivery time for a BT WAN over the last 36 months?	
9.14.	What is the availability SLA for BT WANs?	
9.15.	Is 100% resilience guaranteed, at every point, for BT WANs?	Yes / No
9.16.	What WAN and end point management is included within BT WANs?	
9.17.	Can you provide SIP trunking on BT WANs?	Yes / No
9.18.	Can you provide SIP trunking on Virgin Media WANs?	Yes / No
9.19.	How many BT WANs have you provisioned within the last 36 months?	
9.20.	What is your approximate annual spend with BT?	
9.21.	How many alternative carrier, or hybrid WANs	

	has your company delivered over the last 12 months?	
9.22.	What was the average order to delivery time for alternative carrier, or hybrid WANs over the last 12 months?	
9.23.	What was the average delivery lead time for alternative carrier, or hybrid WANs over the last 12 months?	
9.24.	What was the most delayed delivery time for an alternative carrier, or hybrid WAN over the last 36 months?	
9.25.	What is the availability SLA for your proposed alternative carrier, or hybrid WAN?	
9.26.	Is 100% resilience guaranteed, at every point, for alternative carrier, or hybrid WANs?	Yes / No
9.27.	What WAN and end point management is included within alternative carrier, or hybrid WANs?	
9.28.	How many are included within alternative WAN you have provisioned within the last 36 months?	
9.29.	What is your approximate annual spend included within alternative?	
9.30.	If your solution is ultimately reliant upon a carrier, how do you manage their breaches on SLA?	

10.	Background Information	
ID	Question	Answer
10.1.	How many current clients does your organisation have where you have provisioned or novated the WAN?	
10.2.	How many of the customers receive a managed service from your organisation, similar to CRFCA's requirements?	
10.3.	Based on your proposed solution(s), where would the annual contract value of the CRFCA contract sit in your client base, i.e. Position 34.	
10.4.	Based on your proposed solution(s), where would the total contract value of the CRFCA contract sit in your client base, i.e. Position 26.	
10.5.	What contractual penalties will you agree to for failure to deliver the new WAN within the contracted delivery and handover time?	
10.6.	How will you ensure that the new WAN is delivered conterminously?	
10.7.	How will you ensure that the CRFCA can provide correct notice to the incumbent WAN provider to ensure that there is no overlap with the new WAN, i.e. zero double billing?	

11.	Security	
ID	**Question**	**Answer**
11.1.	How do you propose to secure the WAN environment?	
11.2.	Are you able to include PCI compliance within your proposed solution at no additional cost? If not, what would the cost be to include PCI compliance?	Yes / No Plus cost if not included
11.3.	How will intrusion be detected and prevented?	
11.4.	What will happen in the event of an unauthorised access to the network and to our systems?	
11.5.	If the above occurs, how are the identified risks minimised?	
11.6.	Are you able to manage intrusion detection as part of the service? How will this be facilitated?	
11.7.	Confirm that the design of the WAN, Internet, Firewall and connectivity to our LAN will be undertaken in absolute compliance with Industry Standards, best practice and that the design will be fully documented and shared with CRFCA.	Yes / No

12.	Disaster Recovery	
ID	**Question**	**Answer**
12.1.	Describe your organisation's levels of infrastructure, staff and locations resilience ensuring at all times a continuous service to your clients.	
12.2.	Describe your organisation's approach to Disaster Recovery (DR) for incidents that affect your own organisation, or supply chain.	
12.3.	Describe your organisation's approach to Business Continuity Planning (BCP) for incidents that affect your own organisation, or supply chain.	
12.4.	How would you propose to provide a robust approach to the support of the CRFCA infrastructure, in the event of a disaster impacting their business?	
12.5.	Detail how you would manage and prioritise multiple client DR invocations, such as in the event of a large-scale infrastructure failure impacting adversely impacting upon the operation of your organisation.	
12.6.	How are increases and/or changes to the primary customer environment and DR environment managed from a commercial perspective?	
12.7.	What is the level and frequency of DR and BCP testing that your organisation carriers out?	
12.8.	Are the above tests independently ratified by external third parties?	Yes / No

ID	Question	Answer
12.9.	Provide a copy of your current DR/BCP Plan.	
12.10.	Provide a copy of your most recent test results.	

13.	**Account Management and Service Reporting**	
ID	**Question**	**Answer**
13.1.	Provide a brief summary describing how you would typically monitor the performance of your proposed services. (Maximum 500 words).	
13.2.	Describe your standard Account Management process.	
13.3.	Provide an example monthly service performance report.	
13.4.	What service models do you follow (e.g. ITIL)?	
13.5.	How do you develop and maintain customer relationships?	
13.6.	How do you respond to customer dissatisfaction or failures to meet SLA targets?	
13.7.	How do you ensure that an account team does not have an excessive churn of staff?	
13.8.	There should be a named individual responsible for delivery of this service and a succession plan established, in case the individual is unavailable. Describe how this requirement will be delivered.	
13.9.	There should be a contingency plan in place for key members of the proposed project delivery team. Describe how this requirement be delivered.	
13.10.	Are you willing to formalise limits to account team staff churn contractually?	
13.11.	Would you agree to a contract extension and renegotiation at the 24 month point of the contract?	
13.12.	Please outline your standard reporting following an SLA failure, including report KPIs and root cause analysis.	

14.	**Transition Timescale**	
ID	**Question**	**Answer**
14.1.	Provide a forecast of the transition timescale that you would forecast for a service of this nature.	
14.2.	What notice period would your company require before a service transition could commence?	
14.3.	Would you commit to contractual delivery dates for the provision of a new WAN?	Yes / No
14.4.	What penalties would you propose for failure to meet these delivery dates?	
14.5.	How would you ensure any such failures do not financially impact CRFCA in any way?	
14.6.	How do you manage situations where lines are	

	not available in time to meet a scheduled service go-live dates? For example, if all required lines were in place to deliver the CRFCA WAN service, apart from one that terminated at a smaller regional office location, how would this situation be managed?	

15.	**Implementation Planning**	
ID	**Question**	**Answer**
15.1.	Provide details of the implementation transition planning undertaken for an engagement of this nature.	
15.2.	Tenderers should describe how they would work with the current CRFCA Supplier(s) to ensure the successful delivery of the implementation.	
15.3.	Tenders should describe their approach to the management of risk and provide an initial risk register relating to this project.	
15.4.	Provide details of key tasks and their ownership required for implementation planning.	
15.5.	Provide an implementation plan detailing the typical implementation of an engagement of this nature. The implementation plan should contain a Gantt chart that provides detail of the proposed approach and timescales. (The response to this question must be no longer than 1000 words).	

16.	**Exit Planning**	
ID	**Question**	**Answer**
16.1.	Provide details of the exit planning which would be undertaken for an engagement of this nature.	
16.2.	Provide details of key tasks and their ownership required for exit planning.	
16.3.	At the end of the contract period, is it possible for all services to be novated to an alternative supplier?	Yes / No
16.4.	At the end of the contract period, is it possible for a 90-day extension period to be put in place, if requested by CRFCA? If yes, what would be the commercial calculation for this extension?	
16.5.	Will all carrier contracts be established in a manner that ensures that they are co-terminus?	
16.6.	Will all elements of the CRFCA contract be	

	established in a manner that ensures that they are co-terminus?	

17.	**Executive Summary**	
ID	**Question**	**Answer**
17.1.	Please provide an executive summary of your proposal. (The response to this question must be no longer than 1000 words).	

Financial Response Requirement   Financial Evaluation

Financial Evaluation	Provide a description of your proposed commercial model and costs for delivering these services using the spreadsheet template provided in Appendix K.	

Appendices:

    A.   Supplier Questionnaire, Managed Service Provider *(To be completed by Tenderers)*

    B.   Supplier Questionnaire, WAN Service Provider *(To be completed by Tenderers)*

Lot 1 – Managed Service Provider Appendices:

    C.   Service Requirements (3 parts)

    D.   Current Equipment List

    E.   List of Sites and Numbers of Users

    F.   Call Volume Statistics

    G.   Managed Service SLAs

    H.   List of Equipment for Catalogue Purchases

    I.   Financial Model Template – MSP *(To be completed by Tenderers)*

Lot 2 – WAN Service Appendices:

    J.   Network Diagram (2 parts)

    K.   Financial Model Template – WAN *(To be completed by Tenderers)*

Response Documents *(To be completed by Tenderers)*

    L.   Response Template for Managed Service Provider response

    M.   Response Template for WAN Provider response