Exercise ARMY CYBER SPARTAN 6-8 and STE management Statement of Requirements (SoR)

Ref: 707942451

Introduction

Purpose

1. This SOR provides potential Service Providers (SP) with the requirements for the 13 Signal Regiment (13SR) cyber range over the next 3 years.

2. This SOR informs potential SPs of three distinct packages which will form a single contract.

3. The first package is for the creation and execution of the annual cyber collective training and validation exercise known as Ex ARMY CYBER SPARTAN (ACS). ACS occurs once per year therefore this SOR is for iterations 6 – 8 with execution dates in autumn 2023 and an agreed date in 2024 and 2025.

4. The second package is for full cyber range support of the existing on-premise data centre including a redesign to enable multi-tenancy which will offer greater utility and concurrent use and must include design and development activities in support of cyber simulation, assurance and validation

5. The third package is to offer professional services in order to model 'digital-twins' of 13 SR IT assets to enable virtualising modelling, performance testing and assurance in support of the Cyber Information Services Operating Centre (CyISOC) and the wider MOD Defence Cyber Operations programme.

6. The packages list above are in delivery order. The purpose of Ex ARMY CYBER SPARTAN (ACS) is:

"Ex ACS is to attract, assess, advise and educate Army personnel, developing collective training and cyber capability, in a challenging and realistic cyber environment in order to exploit Defensive Cyber Operation (DCO) KSE aligned to Defence outputs."

7. As an annual and professionalised exercise, a number of specified objectives have been agreed with all stakeholders. These must be achieved in order for the exercise to be considered a success. The top five (specified) objectives of Ex ACS are:

a. To educate, upskill and enhance DCO capability by exploiting equipment, workforce and training in order to inform and enhance the development of future Corps, single service and Defence outputs, collective training and capability.

b. Deliver ambitious, challenging and realistic cyber-security scenarios based on current threats and vulnerabilities faced by Defence and industry.

c. Enhance and Develop working relationships with other Defence and Governmental organisations, including international partners, to foster relationships, participation and innc

d. Attract, talent manage, advise and assess personnel who have potential for wider cyber employability and exploit as future cyber leaders.

e. Develop co-operation with other nations and share best practice.

8. The exercise series will be delivered and executed by 13SR with contracted support. Due to the technical complexity and infancy of organic expertise when delivering a large-scale synthetic and virtualised training environment it has been decided that the provision of the technical architecture is to be outsourced. This document articulates the specific requirements for all technical aspects of the outsourcing to ensure that the requirements and expectations of the exercise delivery team are met.

9. The over-arching requirement is the design and provision of a reliable, scalable, and robust multi-tenant and multi-purpose synthetic training environment. This is essential for the success of any cyber-security exercise and Defensive Cyber Operations military training and de-risking activities.

10. To offer maximum value for money and provide a maximum return on previous investment, any SP proposal must wherever possible reuse existing resources including the 13SR on-premise cyber range.

11. Due to the rapidly evolving requirements of cyber simulation, modelling and training activities within the military, any SP contract proposal must be sufficiently adaptable to allow for realignment throughout the contracted term. It is essential to evolve at the rate of relevance.

Objectives

12. The objective of this SOR is to articulate the requirements for an 'on-premise' Synthetic Training Environment (STE) as per the introduction section. The created training platform is to be:

a. Provisioned to facilitate a Cyber-security competition hosting 350 participants and 180 enabling staff.

b. Future proofed by a multi-tenant scalable design.

c. Automated using open-source scripting language to reduce the Total-Cost-of-Ownership while maximising reusability.

d. Multi-purpose and interoperable as a platform to support and host undefined future tasks which will include digital twins.

Background

13. As part of its continuing development of Defensive Cyber Operations (DCO), the Fd Army is developing its capability in support of actions in the cyber-security domain through training, simulation, and modelling. Whilst the Army Cyber Protection Teams (CPT), Army Cyber Information Services Operating Centre (ACyISOC) and other Defensive Cyber Operations (DCO) functions grow in maturity, it must continue to identify talent and force generate from within its existing pool of resources. Opportunities exist to acquire individual skills although harnessing these within a Collective Training (CT) environment is still pivotal to determining how effectively these skills can be applied in representative situations.

14. The requirement for a STE for cyber-security testing, technical assurance, and large-scale modelling for the modern and technically enhanced Basic Combat Skills (BCS) is an essential step towards establishing a persistent CT capability.

15. The Ex ACS series of activities aims to deliver this and meet the overall exercise aim and subordinate objectives. To achieve this 13SR have been tasked with delivering ACS. To date ACS has been delivered under contract on an annual iteration. This has prevented the

enduring knowledge transfer and has prohibited for the full utility of the STE from being harnessed. The technical delivery of ACS was outsourced as the risk to the business to deliver it organically was too high. An outsourced solution does mitigate the resource overburden from the Regiment relating to the technical challenge of creating and supporting the training environment however it also hinders organic development.

16. Until now ACS has been tendered per event. This annual contractual process has been unnecessarily time consuming and has not enabled sufficient throughlife progression between the ACS iterations due to the annual change of SP. This SOR will invite SP to tender for a 36 month contract that will enable consistency and efficiency of activities that will enable the capitalising of knowledge, experience, and evidence over time.

17. The on-premise datacentre which forms the STE capability was originally purchased to deliver ACS. As a very capable platform, it has been agreed that the STE should be partially redesigned to enable multi-purpose and concurrent activities. This concept is known as multi-tenancy and can include activities such as SOC/NOC validation, sandboxing testing, and modelling of networks. To ensure these additional activities can be undertaken safely and without impacting the delivery of ACS, it is a requirement that the STE is to be reconfigured to support multi-tenancy activities.

18. To operate and engineer the STE datacentre requires significant depth and breadth of Knowledge, Skills and Experience (KSE). 13SR possess the most developed KSE required to deliver a STE however these are still at the embryonic stages. As the KSE are gradually developed within the military, and particularly within 13SR, it is expected that there will be a steady and controlled reduction in the requirement for contracted support.

19. To ensure maximum value for money and efficiency of technical resource this contract will enable the opportunity for SP to accept additional work packages on the STE platform, beyond those listed within this SOR at additional cost to the customer. As this SOR is designed to ensure that the STE is fully supported for 36 months on behalf of 13SR, there is scope to enable additional tests, trials and tenants on the STE as it will already be supported. This will enable smaller contracts which use the STE platform or enhance it without repurchasing the base platform (STE) already owned. These may be tendered as additional contract(s)/work package opportunities as a reduced costs as the base STE hardware and software environment will already be under contract, therefore this offers mutually efficient Value For Money.

Requirements

20. This requirement section will detail the requirements for ACS6-8 and will follow by the wider STE support and maintenance requirements. Although this SOR will detail the requirement for ACS 6, it is to be expected that ACS 7-8 will be of a very similar format (albeit with different ICS/SCADA and OPFOR effects in order to maintain the challenging element of the competition).

Ex ARMY CYBER SPARTAN requirements

21. **Overall Requirement**. This is to be a Fixed Price Contract to provide the detail outlined below:

a. ACS 6-8 hosting environment.

b. Design and implementation of DMZ for hosting of training resources.

c. Training resources.

d. Design for multi-tenancy hosting that can be accredited up to the classification of OFFICIAL-SENSITVE.

e. Delivery of Ex OCULUS ASSURANCE exercise in support of ACS 6-8.

f. Implementation and interfacing of SCADA and ICS connectivity to the network to enable control and monitoring by Blue and Red Teams.

g. The provision for connectivity of additional hardware for testing and development purposes.

22. **ACS 6 hosting environment**. An on-premise VMware STE is required which will deliver the following:

a. Infrastructure for 30 x Blue Teams of 10 personnel operating on each representative enclave. (Scalable up to 60 teams if STE capacity is available via cloud housing or future hardware enhancements).

b. Access to the range for 180 enablers to support functions such as intelligence, targeting, etc.

c. Provide a minimum of 3 tenants.

d. Individualised, role based access for up to 580 personnel at any one time (in a single tenant).

e. The virtualised Simulated Training Environment is to be ready and available for use by Blue and Red Teams for training no later than 90 days before the start of the ACS competition.

23. **Security Domains Breakdown**. Each Blue Team will defend/administer 3 separate Security Domains. Each of the Blue Teams are to be provided with a unique instance of each of the 3 Domains supported by an appropriate Security Operations Centre (SOC) solution to monitor Red Team Opposing Force (OPFOR) effects. Each instance is to consist of up to 20 virtual client terminals and a nominal number of servers appropriate to the scenario. The breakdown of the 3 unique domains are as follows:

a. **Government**: A representative cross-government/coalition network for communication between partners. Within the context of the scenario this may be local or national Government agencies etc. They are to communicate, and access resources hosted within the Grey Space. Architecturally, each Blue Team enclave is to connect to an authoritative root domain in a parent child/hub and spoke topology.

b. **Military**: An independent, autonomous system providing local and interconnected services between each separate Blue Team enclave. Security policies are not to be inherited from a higher domain but instead are to be administered and implemented locally. Consisting of a Client - Server architecture, services provided are to be representative of a typical management information system, e.g. SharePoint, Exchange, Online collaborative communication tools; VoIP, Intranet pages.

c. **Education**: An unclassified, internet (representative Internet) facing network. This is to be representative of an academic or research network. This will typically have internet access and data repositories such as sensitive research, user data stores including academic registration or personal identifiable information.

24. **IP Schema and Routing**. All Security Domain instances created for the Blue Teams are to be configured with IPv4 and IPv6 IP logical addressing and DNS routing (e.g. A and AAAA). The demarcation point between Blue Team responsibility and the Grey Space of each network is to be a Blue Team accessible and configurable router instance (physical or virtual) directly connected to the external interface of the enclave firewall. E.g. this could be a virtual Cisco cloud router connected to the external interface of a PFSense firewall. In this example the router would share the Grey Space routing table however it can be hardened and controlled by the local Blue Team administrators. Other Grey Space intermediary networking devices are not to be configurable by the Blue Teams. The SP is to design an 'in-game' and 'out-of-game' IP and DNS schema. All addressing schemas must be agreed with IC Green Team. The IP schema must have provision for 60 teams, each with 3 enclaves and scalable up to 6 enclaves. IP addressing must be scalable up to 60 teams to allow for future expansion. The IP schema must be managed using an IP Address Management System (IPAM) e.g., Phpipam.

25. **Red Team Opposing Force (OPFOR)**. The SP is to deliver a platform and the suitably qualified and experienced personnel (SQEP) for the purpose of executing OPFOR cyber effects. This must be in support of the exercise scenario. The SP, as lead for the joint delivery of cyber effects, will work in partnership with a nominated Customer Red Team OPFOR. This is to enable the development of the customer's Red Team OPFOR, however the SP must be able to deliver all OPFOR cyber effects, including Red Team Playbooks independently of the Customer. It is therefore to be assumed that all OPFOR deliverables are to be offered by the SP. In order to develop Red Team experience an agreeable number of military personnel will shadow the SP's OPFOR team. This requirement is critical.

26. **Client Builds and Configuration**. The SP is to work in partnership with the Customer to identify client side required software. The Customer is to provide all client hardware including laptops, desktops, monitors and all other peripherals where necessary. All agreed downloadable tools e.g. 3CX softphone, Cisco AnyConnect etc must be hosted within the STE. This will enable a previously unconfigured access terminal with the required software to participate on Ex ACS 6 and engage with all communications services.

27. **Network Cabling**. The SP is to supply all rack and network cabling, Cat 5, Cat 6, Fibre Optic required to connect SP proposed ICS/SCADA and Gamenet support services into the STE.

28. **Accounts and Group Policy**. The SP is responsible for the creation of all Administrator and User accounts in accordance with the Force Element Table which will be provided by the Customer. Group Policy must be applied as necessary to provide a level of realism in terms of system security and administration. This must be applied using Group Policy or a similar process.

29. **Network Access**. The SP is required to provide the configuration for the micro-segmented access to the range for remotely connected users. The SP is to work in partnership with the IC Green Team to create the Cisco configuration required for switches that are to be used by locally connected users, administrators and supporting services. All switches will be provided by the Customer and specifications will be provided to the SP to allow accurate configuration by the SP.

30. **Build of Red Client Area.** As part of the Grey Space, the Red Team OPFOR must have at least 40 customisable Ubuntu jump hosts and the ability to rotate IP addresses and generate further machines on demand. These must be suitably provisioned to enable traffic redirection with minimal performance impact. This area must also host a repository of tools that the Red Team can deploy onto the network.

31. **Remote Access through SSL/TLS encrypted VPN**. The STE is to be easily accessible by on-premise and remote-access users. The minimum viable product must enable micro-segmented access to the hosted environment for 480 concurrent users. Remote access via a secured VPN e.g. Cisco ASA/AnyConnect with valid domain certificate for SSL encryption is essential.

32. **Maintenance of Configuration Management Database**. The SP is to maintain a configuration management database which is to include network diagrams covering the entire system architecture. This is a pre-requisite for meeting the accreditation requirement and must be maintained and updated in all instances. An up to date configuration management and network diagram set allows for easier fault finding during any instances of incidents. The SP will be required to support the Customer with the creation of a security documentation pack including System SyOPs. The Customer will be responsible for the system accreditation process. The SP will be required to assist the Customer throughout the accreditation process.

33. **IPR of System Configuration**. All configuration management material, diagrams and scripts are to be delivered to, and retained by, the Customer. The configuration documentation created throughout the planning and execution of the exercise is to be delivered to the Customer for their retention. Where appropriate a version-controlled copy is to be uploaded to a localised GIT (e.g. Gitlab). Existing STE code, ACS code and design documentation will be made available to the SP for the duration of the contract. The IPR of ACS and the underpinning STE is to be provided to 13 SR.

34. **Blue Team Training** is to be provided to the Blue Team competitors in accordance with the delivered STE. This is to provide competitors a baseline understanding and knowledge of the environment. The SP is to work with the Customer to provide a training pipeline and training activities which will be available from 60 days prior to ACS execution. The preferred training for Blue Team participants would be the delivery of a progressive training pipeline this is to include instructor led lessons and cover defence in depth, the SOC solution e.g. Security Onion, network hardening measures and any critical elements of the tools provided to the Blue Teams. Training on the structure of a Security Operating Centre / Rapid Reaction Team, core skills (SIEM, Hardening etc), incident response and post event recovery.

35. The SP is to:

a. Populate the DMZ with practice CTF and forensic challenges 60 days prior to ACS execution.

b. Work in partnership to identify suitable Immersive Labs activities to assist ACS participants to create a package which can be accessed 60 days prior to ACS execution.

c. Work in partnership with the Customer to identify suitable LinkedIn Learning modules to assist ACS participants which can be accessed 60 days prior to ACS execution.

d. Deliver a Blue Team training package to ACS participants prior to ACS 6-8 execution. (Dates tbc).

e. Deliver Red Team training package to ACS OPFOR members prior to ACS 6-8 execution. (Dates tbc).

f. Deliver Green Team STE familiarisation training package to ACS Green Team prior to ACS 6-8 execution. (Dates tbc).

g. Deliver Green Team STE content creation training package to ACS Green Team prior to ACS 6-8 execution. (Dates tbc).

36. **Red Team Training** is to be provided to the Customer's Red Team OPFOR in accordance with the delivered STE. This is to enable the successful execution of pre-planned and pre-planted exploits in support of the exercise scenario. The minimum training required for the Customer's Red Team OPFOR is the delivery of a training pipeline and a comprehensive Red Team playbook. This must include all specific training required for the execution of pre-planted effects and exploits within the STE.

37. All exploits are to be demonstrated to the customer ahead of ACS execution as a knowledge transfer activity.

38. **Automation and Orchestration of the Exercise Environment**. The master agreed templates required for Blue Team enclaves and WAN infrastructure must be automated and orchestrated using Powershell/PowerCLI and Ansible where appropriate to ensure idempotence, repeatability and deployment from archives. The threshold MVP requires the creation of automation and orchestration scripts to enable the creation of Blue Team VMs and in-game WAN infrastructure.

39. All automation and orchestration scripts are to be delivered to the Customer for their retention.

40. All automation and orchestration scripts are to be explained and demonstrated to the Customer to assist with KSE development.

41. **Naming Convention**. A scalable and hierarchical naming convention is to be used for all configurable items. This is to include physical assets and logical assets including all virtual machines used throughout the in-game environment and the physical STE.

42. **Special Systems**. The following representative SCADA/ICS networks, or similar, are to be modelled either virtually or physical and integrated into the STE. A unique instance of each network is to be created for each of the Blue Teams. Vulnerabilities are to be pre-planted into the SCADA/ICS networks and where possible is to be integrated to have second order effects. E.g. If a HVAC system is compromised and disabled it may trigger a PLINK/PowerCLI script that will in turn disable a VM to demonstrate the reliance between networks. Attack vectors and exploits are to be proposed by the supplier and agreed with the Customer Green and Red Team IC prior to implementation.

a. Heating Ventilation Air Conditioning (HVAC) Systems (alternative negotiable).

b. Power Generation and Distribution (similar to a power solution which may be used within a Brigade / Division HQ) (alternative negotiable).

c. Unmanned Aerial Vehicle / Unmanned Aerial System (alternative negotiable).

d. A scenario enriching distribution system e.g. fuel, water, vaccine, pay etc (alternative negotiable).

e. Recognised Air Picture (alternative negotiable).

f. Railway signalling system.

g. Fuel distribution system.

h. Logistical supply chain.

43. **SCADA Connections**. The virtual/physical connection of the SCADA/ICS networks is to be integrated into the Blue Team enclaves at a network interconnection point conducive to the exercise scenario.

44. **Blue Team Security Tools Repository**. All domains are to allow Blue Teams to install open source tools from an exercise-controlled repository to help them protect and monitor networks after sheep dipping. An example may be the Sysinternals suite of tools. These repositories are to be created within the exercise environment and represent Internet file stores, but not bridge between 'in-game' and 'Internet' at any time without consultation and approval from the Customer.

45. **Sheep Dip solution**. A Sheep Dip solution is required to provide a safe mechanism to impex data to and from the synthetic training environment. This must be provided with up-to-date Anti-Virus.

46. **Green Team Helpdesk support**. The SP is to provide and operate an Incident Management System. This is to support "out of game" fault reporting and resolution of incidents. The requirement is the provision of an incident management system and the full management of all incidents covering L1 - L4. A service desk is to provide both a voice support feature as well as a helpdesk ticketing system. This helpdesk is specific to the ACS instance and does not cover STE datacentre faults.

47. **Reuse of materials.** Where appropriate the Customer may provide access to previously purchased military equipment to ensure value for money. This may include real-estate, server compute and storage, network access devices and cables.

48. **Scoring Solution**. The SP is to provide a mechanism to deliver an automated and configurable scoring system with a dashboard accessible through a web browser. This must enable participants and observers to seamlessly follow the progress of the competition with live scoreboards and overview of incomplete tasks. The minimum requirement for the scoring is a solution providing near real-time visualisation and comparison of competition data. The tool is to be able to illustrate how different participants compare to participant progression over the event. In addition, this is to include a dashboard accessible to all participants displaying a customised view based upon the role of the logged in user. The scoring system must be sufficiently customisable to enable ad-hoc score as well as scoring based upon pre-set criteria and be able to support multiple activities e.g ACS and internal competitions. All scoreboard data is to be exportable in a common format e.g CSV.

49. **Appropriate Network Monitoring Tools** are to be integrated into the Synthetic Training Environment and made available for use and analysis. These are required to measure and record performance metrics of physical hardware and key services e.g. current levels of network traffic, server load and capacity. Example tools include LibreNMS, Observium, SmokePing. The SP is required to use Codenotary Metrics and Logs on STE.

50. **Simulated Network Traffic** is required and to allow simulated attacks to appear more discreet, scripted loading of the user domain services will be provided by the S P. Examples but not limited to include emails, chat and video messaging, internally and externally, automatically created within all domains. Other scripted user traffic will be required to generate noise on the domains. This generator should be able to replicate traffic between each blue team, yellow team and onto/from the grey space – it should be highly configurable and on call from Red Team. All domains will also have a limited number of physical users within them (Yellow Team) that will generate other traffic in order to trigger events. The attacking Red Team OPFOR will have an area to infiltrate the user domains either by directly connecting to

them or via the Grey Space. Each Blue Team should have dedicated Yellow Team users who have a physical terminal to log on to.

51. **The Grey Area** is representative of the WAN infrastructure and is to remain outside of Blue Team control. This is analogous to a pseudo country and typically provides:

a. A variety of pre-planted exploits of varying complexity are to be embedded into the Grey Space and Blue Team enclaves as launch vectors for OPFOR activities in support of the Scenario. The sequence of exploits will be aligned to underpinning exercise scenario and planned exercise activities.

b. Inter-nodal routing between the Blue Teams across all three domains. This is to include multi-AS BGP which will add depth to the virtual network and enable OPFOR obfuscation and the ability to perform network protocol manipulation e.g. BGP path injection, MITM attacks etc.

c. Pre-planted access points for OPFOR activities creating physical/virtual ingress connectors.

d. Structured DNS including root DNS if appropriate.

e. Representative websites to support the exercise scenario.

f. Simulated social media (Twitter, Facebook, 9Gag etc) that allow for:

(1) The conduct of offensive information influence operations.

(2) Social engineering to influence audiences and acquire personal/professional data from key groups/individuals.

(3) The attempted hacking of social media network accounts to sabotage Blue Force activity.

(4) News Websites (BBC, Reuters, Aljazeera, Fox), to support in game activities and underpin the scenario.

(5) A variety of Grey Space web hosted services including a minimum of 30-40 DNS accessible websites, file sharing sites etc are to be created to generate DNS traffic to partially conceal OPFOR activities.

52. **Out of Game** - **GameNet Support and Management Services** will need to have:

a. User areas/workstations, including remotely connected users will require access to real-time communication services (VoIP, VTC etc) in order to support the coordination and the conduct of the exercise. This solution must allow the management of team conferences, bespoke chat rooms etc.

b. Collaborative working area uploading reports, PXR points, SOP/SOI updates. This should include Microsoft SharePoint or a similar solution.

c. A Chat Room portal such as Mattermost must be available for the situation awareness of all team competitors.

d. User guides for all systems must be created in partnership with the Customer and provided to exercise participants for use of tools such as jump servers, Mattermost, VTC, navigating enclaves etc.

e. A live streaming function must be provided to share exercise instructions. E.g. A countdown display to key events.

53. **System Accreditation.** The SP is responsible for assisting the Customer with accreditation of the STE by providing information and schematics on request. As a minimum in terms of accreditation the STE is to be supported by an appropriate Risk Balance Case (RBC) and SyOps endorsed by the appropriate Security Accreditor. The preferred outcome is for the STE to be delivered with full Risk Management Accreditation Document Set (RMADS). It is the responsibility of the project delivery team for the through life management, and to ensure that this accreditation is obtained.

54. All participants and enablers will be required to hold UK or NATO security clearance sufficient to handle up to OFFICIAL-SENSITIVE / RESTRICTED. Personnel who require access to the Land Systems Reference Centre (LSRC) will require UK or NATO SECRET vetting.

55. Following the exercise, the SP must sanitise any SP provisioned equipment used to enable the STE in accordance with HMG IA Infosec Standard 5. This is to be completed with written confirmation received by the Customer prior to the After-Action Review.

56. **Corporate Branding**. To enable the effective advertising of the event the following is to be supplied by the SP:

a. Supply of up to 480 cups, notebooks or similar displaying the Ex ACS logo, the exercise name, and the SP logo. (The design is to be agreed with the Customer).

b. Supply of up to 480 lanyards with ID card holders broken down into the following (The design is to be agreed with the Customer):

(1) 300 light blue lanyards displaying the exercise name printed in white text.

(2) 60 yellow lanyards displaying the exercise name printed in white text.

(3) 60 red lanyards displaying the exercise name printed in white text.

(4) 40 white lanyards displaying the exercise name printed in black text.

(5) 30 green light lanyards displaying the exercise name printed in white text.

57. **Design and implementation of DMZ for hosting of training resources.** The Customer is to design and implement a logical demilitarized zone on the 13SR on-premise STE to facilitate the hosting of RBAC accessible training material and resources via a VPN or local connection. The DMZ and training material must be fully operational at least 70 days prior to ACS 6 execution.

58. **Training resources.** The customer is to pre-load the STE DMZ with complimentary training resources and content. This should include:

a. CTF (KSAT mapped where possible).

b. Forensic challenges.

c. Content hosting environment for customer created content.

d. Reference links.

Requirements

Cyber Range support and development

59. To ensure that the greatest Value for Money is achieved from the cyber range it must be redesigned as a multi-purpose synthetic training environment (STE) which is capable of simultaneously hosting a variety of tasks of different architectures and scales.

60. The redesign and maintenance of the STE is in addition to the Ex ACS requirement. Potential SP should ensure that any proposal in response to the invitation to tender addresses all requirements within this SOR.

61. Potential SP should not submit a proposal that does not address both ACS and support requirements.

Maintenance

62. The STE capability known as the 13SR cyber range is owned by 13SR. This includes inventory items including existing hardware, software, licensing and infrastructure as code (e.g Ansible).

63. 13SR will retain ownership of all STE assets. The responsibility of all STE maintenance tasks will be transferred to the SP under contract.

64. Throughout the 36 month contract period detailed within this SOR there may be customer based business decisions to migrate the STE capability to a hybrid cloud solution or to 'scale up' or to 'scale out' on-premise. The STE inventory and assets, including codebase that form the STE will remain property of 13SR irrespective of the hosting platform solution e.g cloud or on-premise.

65. The SP will be accountable for all maintenance activities. The customer may assist however maintenance will remain the responsibility of the SP.

Daily maintenance

66. All maintenance activities are to be provided by the SP. These are to include:

a. **Physical host** – To identify failure(s) and alert(s) of the STE infrastructure via syslog, ILO, IDRAC, SNMP etc.

b. **Logical host** – To ensure patching and licensing of all devices within the STE inventory including VMware, Cisco, Dell, HP including all gamenet and range support services.

c. **Resolving in-warranty failures** with the associated vendor on behalf of 13SR.

d. **Domain Management**. The SP is to ensure that the STE has a valid domain and a verified SSL certificate for the 36 month contract period.

e. **Rack Management**. The SP is to ensure that good housekeeping is applied to the occupied rack space. This is to include accurate connectivity diagrams and logs.

6 monthly maintenance

67. The SP is to provide 13SR with a health check report of the STE. This is to include:

a. Resource utilisation metrics to enable proactive and pre-emptive capacity planning.

b. The reporting of persistent faults and the impact on STE availability and performance.

c. The recurring faults and the impact on STE availability and performance.

d. Licensing and warranty run out dates.

Technical enhancements

68. The current design of the 13SR cyber range is a single purpose platform to host Ex ACS. Although the existing design provides a highly redundant and highly available VMware based Software Defined Data Centre (SDDC) the hypervisor architecture has been configured as a single tenant which is not capable of hosting simultaneous events on the STE without the risk of data cross talk.

69. There is a requirement to modify the STE design to support technical enhancements that will support concurrent lines of development without the risk of cross talk. This will greatly increase the Return on Investment and Value for Money of the STE.

Multi-tenancy

70. The SP is to provide an STE architecture re-design to enable multi-tenant access for the concurrent planning and execution of activities.

71. The SP is to design and configure a multi-tenancy solution for a minimum of 3 tenants.

72. The multi-tenancy solution is to be scalable beyond 3 tenants in order to support potential future expansion without the requirement for significant redesign. It is assumed that expansion beyond the 3 tenants will require additional storage and compute resources, either on-premise or cloud hosted.

73. The SP is to consult with 13SR and a nominated cloud SP, e.g MODCloud, to identify a technical solution for dynamic cloud integration during periods of on-premise resource exhaustion where ballooning into a cloud provides the most cost effective method of scaling.

Turn Key Solution - Rapid redeployment of existing archives

74. Virtualised environments that have been previously created for use on the STE are to be rapidly re-deployable via a simple GUI menu to enable maximum repeatability of events. It should be possible to redeploy archived templated environments e.g.: ACS5 in a highly automated, low interaction solution.

75. Any proposed redeployment solution must be fully documented by the SP.

76. The proposed “turn key” solution must enable redeployment of future environments that will also be archived e.g ACS6-8.

77. The “turn key” solution is to remain functional and configurable beyond the length of the support contract. The solution may be shared for other SP projects however 13SR must retain this capability post contract cessation.

Near Turn Key Solution – Template modelling

78. The SP is to provide a “minimum viable deployment” solution. This will enable the rapid deployment of a selection of pre-agreed templates for the purpose of modelling. This is a requirement and will enable a Green Team member to create an exercise deployment using a catalogue of templates including, but not limited to:

1. Windows 7
2. Windows 10
3. Windows Server
4. Kali
5. Security Onion
6. CentOS

79. The “near turn key” solution will enable rapid modelling and prototyping and is to be deployable to a designated tenant.

80. Deployable templates used within the “near turn key” solution are to be modifiable and saved as additional templates. E.g a base template of “Windows 10” may be copied and saved as “Windows 10 with Office” installed.

Video Streaming Solution

81. During exercise activities there is a requirement to broadcast a video stream to local and remote users out-of-game. The purpose of the video stream is to enable situational awareness of the exercise. The current solution is a YouTube stream embedded in an on-premise Jitsi conference. The potential SP is to propose an alternative and scalable video streaming solution. E.g AWS Interactive Video Service.

82. Each tenant must be able to stream a different video source during concurrent activities.

Remote Integration Packs to enable dislocated hardware integration

83. To enable physical integration of geographically dis-located systems and services into the STE there is a requirement to provide an IP enabled secure bridge solution using a secure VPN technology to create a logical connection.

84. The proposed solution must allow integration into VMware vCenter/NSX-T.

85. The SP must identify, cost, deliver and configure 3 remote integration packs (RIP).

86. The proposed RIP solution must support the generation of logging and performance metrics. These will be used for the monitoring of service performance and availability.

STE Range Status Dashboard

87. The current STE management suite of tools is feature rich. Although there is a requirement to retain the individual specialist applications for STE administration and engineering there is a requirement to create a simplified high-level STE status dashboard.

88. The STE range status dashboard is to provide the essential information pertaining to the status of the STE and tenant(s) to the viewer. This information should include, but is not limited to:

a. Range status e.g open / closed

b. Range performance e.g compute / storage

c. Bandwidth utilisation of WAN links

d. Jitter/latency/loss of WAN links

e. Clock with start, finish and remaining exercise time.

f. Connected user count

89. The desired solution should have an interactive “range activation” button.

Additional STE enhancements

90. In addition to technical enhancements there is an opportunity to offer greater support for wider Defence. These will support wider Defence projects and policies including the Land Industrial Strategy (LIS) by enabling additional activities.

91. **Academia**. Due to the success of the STE over previous years there are multiple academic and technical groups that wish to learn from the STE. Currently the STE platform is being used to assess the team dynamics within a cyber team. In this example there is a requirement to occasionally discuss the technical architecture and provide raw data to the academic establishments. The SP must be willing to support occasional wider defence research projects.

92. All academic activities will be agreed by 13SR.

93. **DMZ hosting**. To support wider training objectives and learning opportunities there is as requirement for the SP to design and create a DMZ within the STE.

94. The DMZ must be designed to only enable user access to those will a valid user account using an RBAC solution.

95. The DMZ is to be accessible independently of the tenants and is to be able to host a range of services (tbc):

a. **Knowledge repository** e.g bulletin board, forum and links to other resources etc.

b. **Example forensic challenges** (refreshed under contract)

c. **Capture the flag environment**. A CTF is to be independently hosted within the DMZ and a practice environment.

d. **Training material hosting platform**. The SP is to provide a solution for hosting training material. This may include videos, questions, powerpoints etc. The solution is to enable content to be uploaded by approved customer representatives.

Fault reporting and escalation

96. The SP is to provide an online fault reporting solution for out of game range management. E.g. Jira, Remedy etc.

97. As part of the proposal the SP is to suggest SLA response times which to open the dialogue.

98. As the STE will be under a maintenance contract with the SP as detailed within this SOR the fault reporting solution must also allow for the logging of requests. These may include RFIs, technical modifications, technical advice etc.

13 Signal Regiment internal requirements

99. **Simulation and modelling**. Guided by the Integrated Review and in support of ACyISOC there is a requirement to create virtual machine images of the deployable systems supported within 13SR. This is to enable the deployment of representative architectures:

a. to assess the network performance.

b. to allow training and validation testing.

c. to enable sandbox testing.

d. to allow integration of concept technologies.

100. This requirement will require the SP to either modify provided VMs to support ansible configuration or to create a representative VM based on build documentation.

101. The SP is to propose an efficient way of deploying multiple templates for simulation purposes.

NOC/SOC Validation

102. As part of the wider ACyISOC objectives there is a requirement to configure a tenant within the STE to enable large scale validation of Network Operations and Security Operations. The purpose of this is to validate military teams who are in a NOC/SOC role against Defence provided criteria.

103. An example of this would be to generate synthetic traffic to create NOC anomalies, and security incidents to alert SOC personnel. This would be aligned to a test series.

104. To offer greatest VfM the SP may choose to repurpose an archived ACS architecture and replace the Blue Teams with NOC/SOC personnel under validation.

Training

Green Team training

105. The SP is to work with the Customer to provide suitable training content for the Green Team engineers to fully understand the STE architecture and be able to conduct range build activities on the STE. This will include a bi-annual, instructor lead, practical range-build training package to be delivered over the period of a day.
The SP and Customer will discuss training dates and content in advance and agree a delivery method. The Customer will support this through supplementary Green Team training.

106. The SP, upon request and in a mutually agreeable time-frame, is to support additional training and validation activities created within the STE by the Green Team.

Additional business opportunities

107. This contract will secure support for the STE for 36 months. To ensure that maximum Value for Money is achieved this contracted support will also provide the opportunity to use the STE for additional work packages within the multi-tenant environment.

108. Funding for additional business opportunities is not included within the STE support and ACS funding line. Additional work packages are to be funded by the service requester via their commercial and financial lines.

109. 13SR are to be consulted prior to the SP engaging in additional business opportunities to ensure deconfliction of activities.

110. 13SR are to remain the primary customer. Additional business opportunities are to not impact the activities of 13SR.

Outputs/Deliverables/Milestones

111. **ACS 6-8.**

112. **Design and implementation of DMZ for hosting of training resources**

a. The SP is to design and implement a scalable RBAC restricted, internet facing, DMZ to host training resources.

b. The DMZ must be configured with IPv4 and IPv6 addressing.

c. The DMZ must be accessible from the Internet (WAN) and the local (LAN) connected used with valid STE user accounts.

d. The DMZ must be configured to enable granular access control of users, groups and tenants.

e. The DMZ access control must be suitable granular to permit/deny access to individual DMZ hosted services.

f. DMZ services must be fully configured for use 90 days before ACS execute and remain available thereafter.

113. **Design of ACS6-8 to include:**

a. Enclave design

b. ICS/SCADA (with variation between iterations)

c. Topology

d. OPFOR effects

e. External integration

114. **Training resources**

a. The SP is to work with the Customer to provide suitable training content for the Blue Team participants of ACS and planned activities. This will include, but not limited to, a CTF and a forensic challenge that is to be hosted on the STE and accessible by authenticated ACS accounts.

b. The SP is to work with the Customer to provide an exhaustive list of additional training links that are to be advertised within the DMZ.

c. The SP is to work with the Customer to identify a training content pipeline on Immersive Labs. The Customer will logically group and advertise the pipeline. Accounts will be provided to the SP from the Customer for this element.

d. The SP is to work with the Customer to identify a training content pipeline on LinkedIn Learning. The Customer will logically group and advertise the pipeline. Accounts will be provided to the SP from the Customer for this element.

e. All content loaded within the DMZ for the purpose of providing a training resource be retained on the STE beyond ACS6 execution.

f. The SP is to provide a one week Green Team training and knowledge transfer event per annum.

115. **Design for multi-tenancy hosting**

a. The SP is to provide a multi-tenancy architectural design to the Customer that can support in excess of 3 concurrent tenants.

b. Tenants must be able to be populated via automation scripts which load from the on-premise backup server.

c. It must be possible to logically enable/disable access to the Internet, DMZ and other tenants on an individual tenant basis.

d. The SP is to provide a quote for the hardware and software required to form a multi-tenancy environment able to host 3 tenants and operate within VMware Failure-To-Tolerate guidelines and best practices.

e. The SP is to provide a BoM for the additional hardware and software required to fulfil this SOR **no later than 1 Jul 2023**.

f. The SP is to procure the required hardware once the BoM has been agreed with the customer and **no later than 1 Jul 2023**.

g. The SP is to provide an invoice for the hardware/software BoM to 13SR/Army Commercial **no later than 1 Jul 2023**.

h. The SP is to provide an invoice for the design and maintenance support contract **no later than 1 Jul 2023**.

116. **Delivery of support specifically for the following major activities:**

Tbc once on contract	Writing Week 1	Initial collaboration between stakeholders for ACS scenario, objectives and development.
Tbc once on contract	Writing Week 2	Detailed OPFOR effect and scenario integration. Output: Draft MEL for ACS 6 execute.
Once on contract	SSL certificate	The SP is to provide confirmation to the Customer that the wildcard SSL certificate and domain name will remain in place until at least 28 Feb 26.
tbc	ACS MPC	SP is to attend the MPC.
60 days prior to ACS execution.	Training Pipeline released	SP is to ensure the DMZ is available and populated with training material. This is to include CTF, forensic challenge, LinkedIn Learning (list), Immersive Labs (list) and external recommended resources.
60 days prior to ACS execution.	ACS user accounts released	The SP is to provide the customer with user accounts for ACS. Non-Green Team access is to be limited to the DMZ only.
Tbc once on contract	FPC	SP is to attend the FPC and be prepared to brief their proposal.
Tbc once on contract	Blue Team training	The SP is to deliver a Blue Team training package. The delivery is to be recorded and uploaded to the STE-VE DMZ where it can be accessed by ACS participants.
Date tbc. Planned for Summer/Autumn 23	ACS Execute	ACS6 execution. The SP will require a physical presence in UK and be able to deliver Green/White/Yellow/Red effects as agreed with the Customer.
Date tbc. Planned for Summer/Autumn 23	ACS DVD/VIP Day	The SP is to provide a collection of models/displays to add context to the visitors day.
Date tbc. Planned for Summer/Autumn 23	ACS6 reversion	The ACS 6 configuration is to be reverted to the start of exercise where it will be available for access by Blue Team members until (execute + 28 days) for additional consolidation. SP will not be required over this period.
ACS execute + 14 days	Transfer of IPR	All SP delivered product including SSD, Ansible/PowerShell/PowerCLI scripts and Red Team playbooks are to be handed over to the Customer.
tbc	AAR	The Customer will host an After Action Review.
tbc	PXR	Post Exercise Report including Customer and SP observations.

117. **Digital Twin modelling.** The SP is to work with the customer to convert a military owned VM template into an reusable and scalable template using Ansible scripting.

118. The SP is to deliver training as part of the Green Team training package to enable the customer to create a blank Ansible accessible VM template for modelling and simulation activities.

Intellectual Property (IP) Rights (Known as IPR)

119. All design documentation, configuration scripts, network topologies, addressing schemas, playbooks and user guides created for the purpose of Ex ACS are to be transferred and retained by 13SR.

120. All design documentation, configuration scripts, network topologies, addressing schemas, and guides created in support of the VMware hypervisor environment are to be transferred and retained by 13SR.

121. Information contained within Ex ACS documentation or shared with the SP by the Customer in relation to Ex ACS are only to be used for the sole purpose of ACS delivery.

122. The commercial supplier may request to retain information provided for the purpose of or created throughout Ex ACS when explicitly agreed in writing with the exercise coordinating officer.

Government Furnished Supplies

123. The following assets are available for re-use by the supplier. These assets have previously been configured with VMware vCenter, NSX as two clusters (1 x HP using vSAN and 1 x Dell using a physical SAN). If the supplier intends to use these assets, they must include the cost of the necessary licenses within the proposal quote BOM.

ACS /STE Assets				
Servers				
Asset	**Count**	**RAM per server**	**HDDs**	**Remarks**
HP ProlLiant DL380	6	512 GiB	8x 980 SSD	2x Intel ® Xeon Platinum 8153 CPU @ 2.00 GHz, 16 logical CPUs each (32).
HP ProlLiant DL380	2	128 GiB	2x 480 SAS 20x 1.8 TB SAS 2x 300 GB SAS	
DELLEMC R640	9	1 TB	DELLEMC	**Storage on UNITY XT** 2x Intel ® Xeon Gold 6238R CPU @ 2.20 GHz, 16 logical CPUs each (32).
DELEMC R740	1		7x 8 TB SAS	Backup server
DELLEMC UNITY XT	1		60 TB	SAN

Clients				
DELL Inspiron	48			
TOSHIBA	2			
HP Desktops	100			
Thin Clients	20			
HP Monitors	200			For the Desktops
Switches				
Cisco Catalyst 9300 24 ports	21			
Cisco Catalyst 9300 48 ports	7			
Other				
LG Tv	13			

Payment

Payment is in accordance with the G-Cloud 13 Framework agreement, Call-Off order form and Schedule of Requirements.

The SP will provide a one-off BOM for hardware.

Contract management arrangements

In the delivery of requirements detailed in this SOR the SP is expected to enable contract management including delivery of documents and attending meetings as detailed below:

- Detailed project plan for the delivery of the contract proposal, to include key milestones for the delivery on schedule, dependencies, exclusions, assumptions and risks.
- Monthly written progress reports for delivery of the elements detailed within the contract proposal and actions required to proceed as planned to meet project milestones. Also, to include financial breakdown, dependencies, exclusions, assumptions, risks and any issues that will affect the delivery of the contract.
- Monthly virtual meetings (to be organised by the SP) to discuss the content of the written update and to agree next steps.
- Attendance at planning conferences, providing an update on the plan for delivery and its progress, financial breakdown, dependencies, assumptions, assumptions, risks and issues that will affect the delivery of the contract.
- Detailed written invoices covering all costs incurred during the delivery of this SOR and in accordance with the Schedule of Requirements.

End of contract/Exit strategy

Prior to the termination of the contract, the SP is to hand over the following to 13 SR:

Provide written confirmation that all configuration information, test data and exercise data have been appropriately sanitised/deleted in accordance with the information's Security Classification, including the methods used to ensure safe sanitisation/deletion.

Ansible playbooks, Powershell and PowerCLI scripts written for the automation tasks of the STE are to be delivered electronically to enable efficient reuse.

Electronic and hard copy of System Design Documentation, including network configuration diagrams.