701551786

PROVISION OF ADS SECURITY OPERATING CENTRE (SOC) SUPPORT

(DInfoCom/0186)

Statement of Requirement

CONTENTS

1. OUTCOME

1.1 The Army Digital Services (ADS) Security Operating Centre (SOC) Support will provide a cost effective, flexible and scalable cyber security support service that can meet the demands of the ADS SOC. Working alongside the existing in-house team, this support will provide the capability to continue the ongoing content and procedural development and cyber protection of the ADS Army Hosting Environment domain and applications.

2. PURPOSE

2.1 The MoD may be referred to as “the Authority” hereafter.

2.2 The purpose of this document is to define the Security Operating Centre (SOC) Support services required by ADS. This is inclusive of, but not limited to:

2.2.1 On-going cyber protection of the AHE.

2.2.2 Development and upskilling of the existing in-house SOC team.

2.2.3 Use case development in line with existing, new and evolving cyber threats.

2.2.4 Log on-boarding so ensure adherence to Bulk Data controls and GPG13.

3. SOR COMPOSITION

3.1 This document is split into three schedules:

3.1.1 Schedule 1 - Background to the ADS Organisation.

3.1.2 Schedule 2 - The Services required.

3.1.3 Schedule 3 - The Service levels required.

4. HARDWARE AND SOFTWARE INFRASTRUCTURE PROCUREMENT

4.1 The Authority will be responsible for procurement of all the IT assets and equipment required to support this requirement.

5. INTELLECTUAL PROPERTY RIGHTS (IPR)

5.1 The selected Supplier shall not retain IPR relating to any services delivered during the terms of the contract.

6. LICENCING AND SUPPORT AGREEMENTS

6.1 The Authority will retain the overall responsibility for ensuring that all system software utilised by the Service Supplier on behalf of the Authority is fully licenced with the provider.

7. EXIT PLAN

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

8. DURATION

8.1 The duration of the overall requirement is for a twenty-four (24) month period, from 01 Aug 2021 until 31 Jul 2023, with a twelve (12) month option period.

SCHEDULE 1 – BACKGROUND TO THE ADS ORGANISATION

9. OVERVIEW

9.1 This following section is designed to provide information, for context, on the structure, organisation, processes and remit of the Authority. It is therefore broader than the specific needs of this contract which are detailing in the following schedules.

9.2 ADS provides hosting and through life application-based information services to [redacted]. It comprises of a core of 100+ personnel across military, Civil Servants (CS) and core Technical Support staff which includes elements from 605 Signal Troop (10 Signal Regiment) that directly support ADS. This figure increases when new products are in delivery.

9.3 ADS [redacted]. [redacted] capability and is currently provided under a G-Cloud contract. In the [redacted[redacted]; known as the Army Hosting Environment (AHE). The landscape of ADS hosting capability is as detailed on Page 6, Figure 1. In addition to these hosting capabilities, some aspects of the pipeline for delivery onto both the JSF and AHE are in [redacted], enabling remote access to the product teams.

10. THE ARMY HOSTING ENVIRONMENT (AHE)

10.1 The AHE is a 'private cloud' located on MOD premises that currently supports 70+ business applications across multiple security classifications. In the [redacted] environments, [redacted]. ADS provides the hosting platform in the form of a fully Software Defined Data Centre (SDDC) ([redacted]) [redacted].

10.2 The applications hosted on AHE support a wide range of functions across [redacted], [redacted], [redacted], [redacted], [redacted] and [redacted]. These include a number of applications that have been developed by ADS on behalf of the Field Army, the more significant ones of which include:

10.2.1 [redacted]

10.2.2 [redacted]

10.2.3 [redacted]

10.2.4 [redacted]

10.2.5 [redacted]

10.2.6 [redacted]

10.2.7 [redacted]

10.3 More broadly there are currently 70+ live application services on the [redacted]; [redacted], [redacted]. [redacted].

10.4 The Army also has a significant Management Information (MI) and Business Information (BI) capability in the form of the [redacted] and [redacted], to provide reporting and analytics across the Army. [redacted], there are 6 application services. This is anticipated to grow due to the [redacted].

10.5 Application users range from a handful for some of the more specialist applications to tens of thousands for those widely used [redacted], [redacted], [redacted].

10.6 ADS is now moving to an [redacted]. As applications are being improved or delivered the opportunity is being taken to break down existing applications into their component parts and delivered as business services.

10.7 ADS are also looking into the use of [redacted] allowing centralised management and interoperability between applications and services that [redacted].

[redacted]

Figure 1 – AHE Landscape

11. THE JOINT SERVER FARM (JSF)

11.1 The JSF is a 'public cloud' currently hosted by Rackspace and is contracted as Infrastructure as a Service (IaaS). The JSF provides the hosting capability for the [redacted] that support 300,000 registered users across [redacted]. [redacted] but can also access them from the [redacted]. It also provides Defence with a platform to host other capabilities, these include [redacted] amongst the 19 partners.

11.2 The DGW provides an official capability that is accessed via [redacted] behind which there are currently 26 services of which [redacted]. These are predominantly [redacted]with a handful of native [redacted]. The [redacted] range [redacted], [redacted] and [redacted]. The bespoke developed services include, [redacted] and [redacted] and [redacted]. [redacted].

12. OPERATING MODEL

12.1 ADS has invested significant time and effort to adopt Agile and then start to mature as a DevSecOps organisation. A pipeline approach has been established for deploying onto both the AHE and the JSF, utilising the same technologies for the majority.

12.2 The product teams are utilising Continuous Integration (CI) and Continuous Deployment (CD) with SCRUM as the agile framework. The in-service team have adopted Kanban. A Significant and on-going investment has been made to automate testing.

12.3 The Service Operations and Management teams utilise ITIL for change, incident, problem, knowledge and asset management. Remedy is used as the main IT Service Management Tool. The change and incident processes are used to capture the requirement but are then fed into the DevSecOps ways of working.

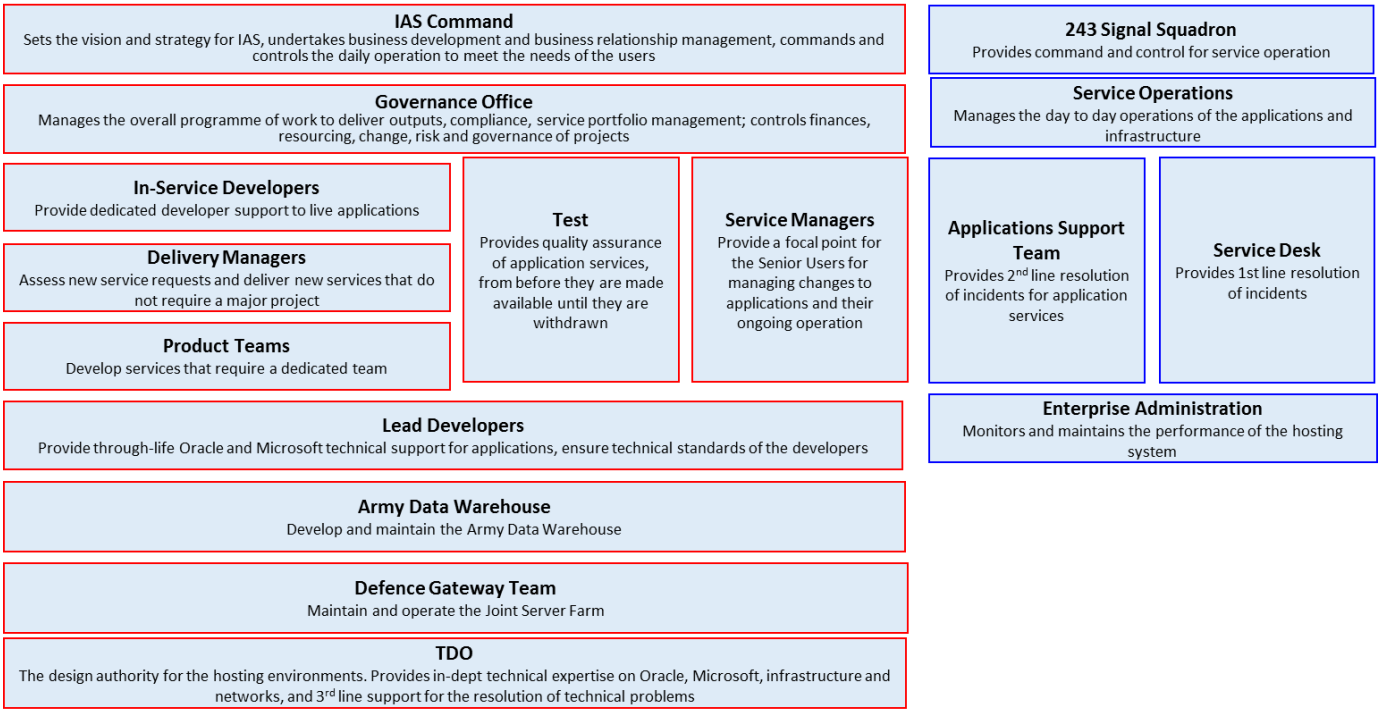
12.4 The Service landscape on AHE is as detailed below in Figure 2.

[redacted]

Figure 2 – Service landscape on AHE

13. ADS ORGANISATION, ROLES AND RESPONSIBILITIES

13.1 The structure of ADS and 605 Signal Troop is detailed in the diagram below and in the following paragraphs:



13.1.1 **Product Teams.** These are based predominantly on a 4-6 resource team, comprising of 2-4 developers, 1-2 testers, and a Business Analyst (BA) as their primary skills but all are multi-disciplined. These teams use SCRUM as their main framework for delivering software.

13.1.2 **In-Service Development Team.** These consist of 3 Oracle APEX and 2 .Net Developers with 3 testers matrix managed to enable the Service Managers to make changes to the services they support. These work on bug fixes and minor changes to live services. As the code base is changed the automated scripts are updated. Kanban is the agile framework used to process work. The Service Development Team also provide 3rd line support for the resolution of incidents and problems with application services. ADS has the ability to provide remote Dev/Test for this team utilising Azure. The main Dev/Test is on AHE v2 with automated release on to production.

13.1.3 **Test.** ADS has shifted left with testers imbedded in the product and in-service management teams. These testers are responsible for the automation of the functionality and regression testing. As part of the CI pipeline, after Dev/Test the next phase is System Integration Testing (SIT), where the software is tested on as close to production environment as possible; on SIT integration and exploratory testing are conducted; as well as the assurance of the automation tests. The technical assurance is provided by a senior tester.

13.1.4 **[redacted].** [redacted]

13.1.5 **Defence Gateway Team.** This is a small DevSecOps team that does everything from supporting the infrastructure, to developing new services and maintaining them on the [redacted]. Services include [redacted]. The team has normally undertaken its own testing but has recently had a tester embedded to follow the same operating model as the rest of ADS with a pipeline of environments and automated testing. At present a single tester has been dedicated to this team. The DGW team utilise [redacted] with production currently being delivered via Rackspace.

13.1.6 **Enterprise Administration.** A team of predominantly military (from 605 Troop) and civil servants with some Technical Support contractors. This team supports the AHE v2 for the Official Sensitive and Secret Environments. Responsibilities include support and maintenance of the storage, network, compute, hardware VMware tech stack (including virtualised network), VMs, OS and monitoring the health of applications/services. For all technical matters they are supported and guided by the TDO.

13.1.7 **Service Desk.** A team of civil servants and military that provide the first line of support for applications. This Service Management as a Service requirement will work alongside this in-house capability.

13.1.8 **Service Management.** A team of civil servants and military that ensure that applications continue to satisfy the evolving needs of the business and to support their Business-as-Usual. This Service Management as a Service requirement will work alongside this in-house capability.

13.1.9 **Application Support Team (AST).** This a team of mainly Civil Servants with technical support contractors. The main role of the team has been the transition of services onto Pre-Production and Production and provide second line support for application incidents and problems. The transition of services is now being automated utilising Microsoft Release Manager.

13.1.10 **Technical Design Office (TDO).** This is the main technical hub of the organisation, with the technical expertise for all the technologies employed by ADS. They are responsible for deploying new infrastructure services, handing over knowledge to the relative teams and providing 3rd and 4th line support for these services, predominately infrastructure and main core services for the data centres.

13.1.11 **Delivery Managers.** The delivery of new or small to medium sized services within ADS is the responsibility of Delivery Managers; this could be anything from an infrastructure change to a small product/service.

13.1.12 **Compliance Team.** Provides in-house advice to ensure ADS adheres to security and policies as laid out in Joint Service Publication (JSP) 440 and 604, ISO 27001 and security architecture.

13.1.13 **Configuration Team.** Responsible for the configuration control of hardware, software and documentation.

13.1.14 **Security Operations Centre.** Responsible for the protective monitoring of the AHE (O & S).

13.1.15 **Army Data Analytics.** The Army Data Analytics Team offer a range of analytical services to enable the business to gain insight and benefit from enterprise data. Dashboards display data visualisations of the current and historical status of metrics and key performance indicators for the enterprise.

SCHEDULE 2 – SERVICES REQUIRED

14. OVERVIEW OF REQUIREMENT

14.1 To conform to Defence Assurance and Information Services (DAIS) security accreditation agreements for the Army Hosting Environment (AHE), ADS and 605 Network Ops Troop has established a Security Operations Centre (SOC) to monitor and detect real-time activity on the AHE to protect against internal and external threats. Work is ongoing to ensure the SOC can effectively monitor the AHE (OS), (S), (O), and (SDLC) environments to ensure the SOC remains compliant with DAIS.

14.2 Outputs will include but are not limited to; developing Cyber Incident Management and Response plan, Review and develop on-boarding process and procedure for IaaS, PaaS and SaaS, Use Case and content creation and training and development of the existing SOC team. The service needs to be undertaken by technical outputs who hold MOD Security Clearance (SC) as a minimum, with a strong technical background and a very good understanding of Cyber Security compliance, policy and practices.

15. DELIVERABLES

15.1 The high-level deliverables for the service are outcomes associated with:

15.1.1 **Build/Develop Use Cases –** Develop use case and facilitation, threat modelling and transalation of operational requirements into SOC SIEM tool. Focus on insider threat and Data Loss Prevention use case to demonstrate the process used by SOC analysts.

15.1.2 **Cyber incident response plan** – Develop the AHE Cyber Incident Response Plan in line with NIST and SANS guidance and incorporating the wider ADS teams. Create supporting documentation and guidance for SOC and ADS to follow OOH with clear lines to resolver group support.

15.1.3 **SOC Roadmap development** – Develop SOC in line with recommendations from the AHE SOC SOMA report Sept 2020 with focus on SOC reaching its required maturity level of 3.

15.1.4 **IaaS, PaaS and SaaS On-boarding** – Work with wider development teams and develop process for log on-boarding and develop costing model for SOC.

15.1.5 **Official 'O' and Software Design Life Cycle 'SDLC' scope out** – Review of network diagrams of both environments and prioritise log on-boarding into the SOC SIEM tool. Break down of workable project sizes and raise CRQ's with dependant teams for on-boarding.

15.1.6 **Develop SOC BCDR** – Review existing documentation for the SOC BCDR and ADS/Army HQ and develop process/plan that feeds into the wider process.

15.1.7 **Cyber Incident Investigation/Escalation** – Reviewing event channel and MODcerts and identifying issues for escalation to different teams in ADS.

15.1.8 **Training and development** – Mentor existing SOC team and develop play books and training and development content to enable quick upskilling of new starters to the SOC.

15.2 Initially ADS require additional resources to supplement the existing in-house SOC Team. As a guide Table 1 provides a breakdown of the scale of effort likely to represent the initial requirement at contract commencement. Considering the level of autonomy and velocity that ADS requires, and again presented as a guide, the Authority would anticipate the annotated minimum SFIA levels against each role as stated in Table 1. However, the determination of the specific roles, team structure and associated SFIA levels of the technical resources that are to be engaged in delivering this capability is to be determined by the individual service provider so as to maintain this capability as a service.

Ser	Role	Expected minimum FTE	SFIA[1] Level
1	Security Administration	1	5
2	Information Security	1	4

Table 1 – Minimum FTE Resource Structure

16. ESSENTIAL SKILLS AND EXPERIENCE

16.1 Overall, the Authority's requirement is for outcomes likely to be delivered by poly-skilled resource and the following details the skills and experience which are mandatory to ensure the Supplier can meet the Authority's current and potential future requirements for this requirement:

16.1.1 Strong knowledge Cyber Security, with a focus on operational security. Such as security monitoring and alerting, vulnerability management and incident response. Producing supporting security documentation in co-ordination with stakeholders.

16.1.2 A good all-round knowledge of IT systems and Networking.

16.1.3 Experienced in both updating and creating operational security processes and procedures.

16.1.4 Comprehensive experience of working in Security Operations Centres (SOC), with additional knowledge and experience to support junior colleagues within the SOC.

16.1.5 Effective communication skills being able to deliver technical conversations and presentations to a range of different stakeholders.

16.1.6 Network and application security and architecture, incident response, forensic investigation and business continuity management.

16.1.7 Knowledge of various Cyber Security Frameworks, Data Protection and bulk data controls.

16.1.8 Hands on experience with security tooling such as SIEM and EDR solutions. Technical ability to operate them from both an analyst and

[1] Skills Framework for the Information Age - https://www.sfia-online.org/en

engineering perspective. (Monitoring, Use Case and content creation, upgrades and troubleshooting.

16.2 Desirable skills and experience of resources supplied are to be:

16.2.1 Professional certification such as GIAC GCIH, CISSP, CISM or ISO 27001.

16.2.2 Experience working in a Defence environment.

16.2.3 Experience of managing and/or mentoring technical personnel.

16.3 Knowledge of on-boarding new log sources into a SOC for security monitoring, while exploring relevant Use Cases for the respective log sources. Where requested the Supplier would be expected to justify SFIA levels of resources utilised in this work in terms of professional memberships, training, qualifications/certifications and above all examples of prior work and experience that is relevant to the role(s) they are assigned against.

16.4 The Supplier and the resources it provides must be free of any commercial ties or obligations to any hardware or software vendors.

16.5 The Supplier will be required to provide a client interface to agree business prioritisations and deliverables.

16.6 It is desirable that resources have current working knowledge of MoD systems and networks and have evidence of previously providing services to MoD or security services.

17. LOCATION

17.1 The normal place of work for this requirement is [redacted]. Although a proportion of this work will be suitable for remote working, under an agile approach there will be routine occasions where team collaboration is essential, as is engagement with the user community, and ADS departments. As such it is not considered to be appropriate that this requirement is satisfied by off-shore resources working outside the U.K.

18. SCALING

18.1 The ability for the Authority to scale up or down rapidly is a key requirement in order to respond to the dynamic needs of ADS, including the ability to resource urgent operational requirements. As such, and subject to demand and budget, the Authority requires the ability to scale up and down the resource requirements in relation to outputs. In essence, this means that there will be a minimum (core) level below which the quantity of outputs will not fall and beyond this a discretionary level that the Authority may choose to exploit in part or whole at various stages throughout the contract.

18.2 The requirement for the provision of additional resources would take 2 forms:

18.2.1 **Additional roles (expansion)** - if an initiative requires a new/further set of skills. For example, a new application is developed for which the outputs commensurately require a new Security Assurance Co-ordinator capability to be established. This would be over and above the current 'on-going' outputs and resource provision.

or,

18.2.2 **Replacement of a role (re-prioritisation)** - if there is need to pivot outputs in response to the Authority's demands which may require a different skill-set. For example, as the expansion of a particular application evolves there is a need to re-balance the resources associated with it. In this example this could be the provision of an additional Level 1 resource at the expense of an alternative resource (or vice versa).

18.3 The Authority will require confirmed rate cards for the provision of resources to deliver new work. This would involve the ability to select pre-defined service offerings in relation to new outputs that would be above the core service. Due to budgetary constraints it is envisaged that the service would be on a capped T&M basis that would enable the Supplier to confirm a maximum cost to meet the outputs required over a set period.

18.4 Although the requirement will not fall below the minimum level of the contract the Authority may also require discontinuing of certain activity at its discretion which in turn may lead to exit (off-boarding) of certain resources.

SCHEDULE 3 – SERVICE LEVELS

19. PROVISIONING

19.1 The Service Supplier is expected to use their 'best endeavours' to provide resources to meet the priorities specified by ADS. Specifically:

19.1.1 Provision of further resources within twenty-five (25) calendar days.

19.1.2 Exit of current resources no longer required within seven (7) calendar days.

20. SECURITY REQUIREMENTS

20.1 All outputs that fulfil this requirement will need to have a minimum level of Security Clearance and be subject to vetting. The minimum standard is MOD Security Clearance (SC), although on occasion the Authority may prescribe a higher level of Security Clearance. This will be applied on a case-by-case basis to both existing and new resources where the Authority has the requirement to do so. The Service Supplier warrants that all staff used to supply their service hold current, MOD applicable, Security Clearances at SC level or above and are willing and eligible to obtain higher clearance levels if the role requires it.

21. CONTINUOUS IMPROVEMENT

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

21.2 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.