**ATTACHMENT 3**

**STATEMENT OF WORK**

|  |  |
| --- | --- |
| **Nominated Candidate** |  |
| **Role** | System Administrator – Multiple Positions |
| **Contract Commencement Date** | ASAP  |
| **Contract Expiry Date** | Contract terms between 12 and 24 months will be considered. |
| **Purpose of Services:** | Professional Services (Clause 7.11). |
| **Role Description** | SIGINT and Network Operations Group – Systems Project Office (SNO-SPO) within the Australian Signals Directorate (ASD), will deliver cutting edge capabilities to Defence through a variety of different programmes and projects. To facilitate this ASD has a requirement for a System Administrator.The System Administrator is required to provide system administrative support under general direction in a key capability domain responsible for the production and sustainment of digital signals processing and embedded platforms. |
| **SFIA Level of Responsibility Required** *Description Below* | The Specified Person will be expected to demonstrate attributes of SFIA Level of Responsibility 4. |
| **SFIA Skills Required***Description Below* | ITOP 4CFMG 4SYSP 4SINT 3RELM 4PBMG 4PROG 3  |
| **Other Skills and Knowledge*****Some or all*** *of the following are required* | **Statement of Suitability Against Other Skills and Knowledge** |
| 1. Automation tools such as Ansible/Puppet, Packer, Kickstart
 |  |
| 1. Network administration – experience configuring routers, switches, DHCP servers
 |  |
| 1. Containerisation familiarity
 |  |
| 1. Familiarity of Continuous Integration/Continuous Delivery (CI/CD) pipelines.
 |  |
| **Major Responsibilities:**  | **Statement of Suitability Against Major Responsibilities** |
| 1. Install and configure ICT infrastructure (physical and cloud managed) – this includes servers and/or network devices
 |  |
| 1. Improve and maintain reliability of ICT infrastructure – this includes configuration automation, upgrading and patching, monitoring, along with utilising version control systems
 |  |
| 1. Transitioning systems and services to corporately managed cloud infrastructure
 |  |
| 1. Fault finding and troubleshooting ICT infrastructure in relation to items 1 – 3 of the Major Responsibilities
 |  |
| 1. Maintain technical documentation in accordance with industry standards
 |  |
| **Other Features of the Role (e.g. location, travelling, shift hours,)** | **Service Provider Response** |
| 1. The role is based in Canberra with minimal travel.
 |  |
| Prepared by: Emma NooneDate: 21/06/2021Authorised by: Tristan Kemp |
| **SFIA Core Competencies** |
| **SFIA Level Of Responsibility 4**  |
| **Autonomy** | Works under general direction within a clear framework of accountability. Exercises substantial personal responsibility and autonomy. Plans own work to meet given objectives and processes. |
| **Influence** | Influences customers, suppliers and partners at account level. May have some responsibility for the work of others and for the allocation of resources. Participates in external activities related to own specialism. Makes decisions which influence the success of projects and team objectives. Collaborates regularly with team members, users and customers. Engages to ensure that user needs are being met throughout. |
| **Complexity** | Work includes a broad range of complex technical or professional activities, in a variety of contexts. Investigates, defines and resolves complex issues. |
| **Knowledge** | Has a thorough understanding of recognised generic industry bodies of knowledge and specialist bodies of knowledge as necessary. Has gained a thorough knowledge of the domain of the organisation. Is able to apply the knowledge effectively in unfamiliar situations and actively maintains own knowledge and contributes to the development of others. Rapidly absorbs new information and applies it effectively. Maintains an awareness of developing practices and their application and takes responsibility for driving own development. |
| **Business skills** | Communicates fluently, orally and in writing, and can present complex information to both technical and non-technical audiences.Plans, schedules and monitors work to meet time and quality targets.Facilitates collaboration between stakeholders who share common objectives.Selects appropriately from applicable standards, methods, tools and applications.Fully understands the importance of security to own work and the operation of the organisation. Seeks specialist security knowledge or advice when required to support own work or work of immediate colleagues. |
| **SFIA Professional Skill Level Description**  |
| ITOP 4 | Provides technical expertise to enable the correct application of operational procedures. Uses infrastructure management tools to determine load and performance statistics. Contributes to the planning and implementation of maintenance and installation work, including building and configuration of infrastructure components in virtualised environments. Implements agreed infrastructure changes and maintenance routines. Configures tools to automate the provisioning, testing and deployment of new and changed infrastructure. Identifies operational problems and contributes to their resolution, checking that they are managed in accordance with agreed standards and procedures. Provides reports and proposals for improvement, to specialists, users and managers. |
| CFMG 4 | Proposes and agrees the configuration items (CIs) to be uniquely identified with naming conventions. Ensures that operational processes are in place to maintain secure configuration, consistent classification and management of CIs, and for the verification and audit of configuration records. Develops, configures and maintains tools (including automation) to identify, track, log and maintain accurate, complete and current information. Reports on the status of configuration management. Identifies problems and issues and recommend corrective actions. |
| SYSP 4 | Reviews system software updates and identifies those that merit action. Tailors system software to maximise hardware functionality. Installs and tests new versions of system software. Investigates and coordinates the resolution of potential and actual service problems. Prepares and maintains operational documentation for system software. Advises on the correct and effective use of system software. |
| SINT 3 | Defines the software modules needed for an integration build and produces a build definition for each generation of the software. Accepts completed software modules, ensuring that they meet defined criteria. Produces software builds from software source code for loading onto target hardware. Configures the hardware and software environment as required by the system being integrated. Produces integration test specifications, conducts tests and records and reports on outcomes. Diagnoses faults and records and reports on the results of tests. Produces system integration reports. |
| RELM 4 | Assesses and analyses release components. Provides input to scheduling. Carries out the builds and tests in coordination with testers and component specialists maintaining and administering the tools and methods – manual or automatic - and ensuring, where possible, information exchange with configuration management. Ensures release processes and procedures are maintained. |
| PBMG 4 | Initiates and monitors actions to investigate and resolve problems in systems, processes and services. Determines problem fixes/remedies. Assists with the implementation of agreed remedies and preventative measures. |
| PROG 3 | Designs, codes, verifies, tests, documents, amends and refactors moderately complex programs/scripts. Applies agreed standards and tools, to achieve a well-engineered result. Collaborates in reviews of work with others as appropriate. |