**ATTACHMENT 1**

**STATEMENT OF WORK**

|  |  |
| --- | --- |
| **Nominated Candidate** |  |
| **Role** | Security 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 Security Administrator.The Security Administrator is required to assist the Program area to develop and integrate software employing an Agile Software Development Methodology (SDM) including; developing software, integrating Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) software, documenting technical processes and assisting with testing and deployment. The successful candidate will need highly developed software development skills and a proven ability to work within an integrated team of technical/non-technical personnel. |
| **SFIA Level of Responsibility Required** *Description Below* | The Specified Person will be expected to demonstrate attributes of SFIA Level of Responsibility LOR 4 |
| **SFIA Skills Required***Description Below* | SCAD 4PROG 3ITOP 3 |
| **Other Skills and Knowledge** | **Statement of Suitability Against Other Skills and Knowledge** |
| 1. Demonstrated experience with network security technologies from vendors such as Palo Alto, Cisco, Sourcefire, FireEye, Blue Coat, Gigamon and Ixia.
 |  |
| 1. Experience in a Security Operations Centre (SOC) including security monitoring and incident response.
 |  |
| **Major Responsibilities:**  | **Statement of Suitability Against Major Responsibilities** |
| 1. Maintain security administration processes and check that all requests for support are dealt with according to agreed procedures.
 |  |
| 1. Provide guidance in defining access rights and privileges.
 |  |
| 1. Investigate security breaches in accordance with established procedures, recommend required actions and support follow up to ensure these are implemented.
 |  |
| 1. Carry out agreed operational procedures, including network configuration, installation and maintenance and patching of network security systems.
 |  |
| 1. Develop scripts or small programs, in software languages such as Python or Bash, to automate business processes and integrate existing security tool and appliances.
 |  |
| 1. Use network management tools to collect and report on network load and performance statistics.
 |  |
| 1. Contribute to the implementation of maintenance and installation work.
 |  |
| 1. Install and configure COTS network security devices such as Next Generation Firewalls (NGFW), Intrusion Detection Systems (IDS), NetFlow and Network Visibility appliances.
 |  |
| 1. Manage alerting and reporting from network security systems.
 |  |
| 1. Integrate security devices with Splunk and create security-related reports and alerts.
 |  |
| **Other Features of the Role (e.g. location, travelling, shift hours,)** | **Service Provider Response** |
| 1. The role is based in Canberra with minimal to no travel.
 |  |
| Prepared by: Darrell MaloneDate: 15/12/2020Authorised by: Travis Alexander |
| **SFIA Core Competencies** |
| **SFIA Level Of Responsibility (LOR 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 |
| **Complexity** | Work includes a broad range of complex technical or professional activities, in a variety of contexts. Investigates, defines and resolves complex issues. |
| **Business skills** | Selects appropriately from applicable standards, methods, tools and applications. Communicates fluently, orally and in writing, and can present complex information to both technical and non-technical audiences. Facilitates collaboration between stakeholders who share common objectives. Plans, schedules and monitors work to meet time and quality targets. Rapidly absorbs new information and applies it effectively. Maintains an awareness of developing technologies and their application and takes some responsibility for driving own development. |
| **SFIA Professional Skill Level Description**  |
| **SCAD 4** | Maintains security administration processes and checks that all requests for support are dealt with according to agreed procedures. Provides guidance in defining access rights and privileges. Investigates security breaches in accordance with established procedures and recommends required actions and supports / follows up to ensure these are implemented. |
| **PROG 3** | Designs, codes, tests, corrects, and documents moderately complex programs and scripts from agreed specifications and subsequent iterations, using agreed standards and tools. Collaborates in reviews of specifications, with others as appropriate. |
| **ITOP 3** | Carries out agreed operational procedures, including network configuration, installation and maintenance. Uses network management tools to collect and report on network load and performance statistics. Contributes to the implementation of maintenance and installation work. Uses standard procedures and tools to carry out defined system backups, restoring data where necessary. Identifies operational problems and contributes to their resolution. |