**ATTACHMENT 1**

**STATEMENT OF WORK**

|  |  |  |
| --- | --- | --- |
| **Nominated Candidate** | |  |
| **Role** | | IT Security Practitioner (Security Architect and Accreditation) |
| **Contract Commencement Date** | | Upon execution of the contract by both parties. |
| **Contract Expiry Date** | | Twelve months from the date of execution of the contract by both parties. |
| **Purpose of Services:** | | Professional Services (Clause 7.11) |
| **Role Description** | | IT Security Practitioner (Security Architect and Accreditation) |
| **SFIA Level of Responsibility Required** | | The Specified Person will be expected to demonstrate attributes of SFIA Level of Responsibility 4 (minimum) |
| **SFIA Skills Required** | | SCTY 4 |
| **Other Skills and Knowledge** | | **Statement of Suitability Against Other Skills and Knowledge** |
| 1. Demonstrated experience in completing system accreditation, in accordance with the ISM. | |  |
| 1. Demonstrated technical aptitude in secure system design (including cloud, container and Windows based environments). | |  |
| 1. Experience applying Govt IT security policies (e.g. ISM, PSPF and E8) and developing internal security policies or procedures. | |  |
| 1. Demonstrated ability to communicate effectively, including concise technical writing skills. | |  |
| 1. Experience in performing system monitoring for security incidents and assisting in incident response activities, as required. (Desirable) | |  |
| 1. Experience in developing and sustaining IT security systems, including DMZ gateway or cross-domain environments. (Desirable) | |  |
| 1. Relevant industry training or qualifications, such as IRAP, CISSP, CISM, CRISC, SABSA, etc. (Desirable) | |  |
| **Major Responsibilities:** | | **Statement of Suitability Against Major Responsibilities** |
| 1. Primary role is to **support the secure design, build and sustainment of ONI IT capabilities**. As part of an agile team applying DevSecOps principles, support projects to deliver systems with the appropriate level of security assurance and risk management. Technology scope is varied, but spans Cloud (Azure and AWS), PaaS (Kubernetes and Docker) and On-Prem (Windows-based). | |  |
| 1. Undertake day-to-day IT system accreditation activities. Scope is varied and will include TOP SECRET through to PROTECTED accreditation activities. | |  |
| 1. Support the maintenance of IT security policies and procedures; identify gaps and prepare updates as needed and well as modernise security awareness material. | |  |
| 1. Support the IT Security section in preparing information briefs and reports. | |  |
| 1. Assist the ONI Incident Response and Security Operations Centre functions, as required. | |  |
| 1. Other tasking in support of the ONI cyber security mission. | |  |
| **Other Features of the Role (e.g. location, travelling, shift hours,)** | | **Service Provider Response** |
| 1. Not applicable | |  |
| Prepared by: Andrew Hanson  Date: 23 June 2021  Authorised by: J. Turner | | |
| **SFIA Core Competencies (V6)** | | |
| **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. | |
| **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** | | |
| SCTY 4 | Explains the purpose of and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls. Performs security risk, vulnerability assessments, and business impact analysis for medium complexity information systems. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate. | |