**ATTACHMENT 2**

**STATEMENT OF WORK**

|  |  |  |
| --- | --- | --- |
| **Nominated Candidate** | |  |
| **Role** | | IT Security Practitioner (SOC Analyst and Incident Response) |
| **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 (SOC Analyst and Incident Response) |
| **SFIA Level of Responsibility Required** | | The Specified Person will be expected to demonstrate attributes of SFIA Level of Responsibility 3 (minimum) |
| **SFIA Skills Required** | | SCTY 3 |
| **Other Skills and Knowledge** | | **Statement of Suitability Against Other Skills and Knowledge** |
| 1. Demonstrated experience in performing the functions of a Security Operations Environment; performing system monitoring for security incidents and assisting in incident response activities. | |  |
| 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 writing skills. | |  |
| 1. Experience in sustaining IT security systems, including vulnerability analysis tools. (Desirable) | |  |
| 1. Demonstrated technical aptitude in secure system design (including cloud and Windows environments). (Desirable) | |  |
| 1. Understanding of the system accreditation process, per the ISM. (Desirable) | |  |
| 1. Relevant industry training or qualifications, such as GIAC, CISSP, etc. (Desirable) | |  |
| **Major Responsibilities:** | | **Statement of Suitability Against Major Responsibilities** |
| 1. Primary role is to support the IT Security section in the ONI **Incident Response and Security Operations Centre function**.  * Collaborate with System Admins to generate logs and develop incident use cases. * Using existing SIEM tools, build alerts, dashboards and automated reports. * Provide day-to-day monitoring of SIEM data. * Initiate Incident Response activities as required. | |  |
| 1. Support the IT Security section in preparing information briefs and reports. | |  |
| 1. Support the maintenance of IT security guidelines and procedures; identify gaps and prepare updates as needed. Aid in modernising security awareness material. | |  |
| 1. Contribute to IT system accreditation activities, as required | |  |
| 1. Apply DevSecOps principles to support the secure design, build and sustainment of ONI IT capabilities. | |  |
| 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 3** | | |
| **Autonomy** | Works under general direction. Uses discretion in identifying and responding to complex issues and assignments. Usually receives specific instructions and has work reviewed at frequent milestones. Determines when issues should be escalated to a higher level. | |
| **Influence** | Interacts with and influences colleagues. Has working level contact with customers, suppliers and partners. May supervise others or make decisions which impact the work assigned to individuals or phases of projects. | |
| **Complexity** | Performs a range of work, sometimes complex and non routine, in a variety of environments. Applies methodical approach to issue definition and resolution. | |
| **Business skills** | Demonstrates an analytical and systematic approach to issue resolution. Takes the initiative in identifying and negotiating appropriate personal development opportunities. Demonstrates effective communication skills. Contributes fully to the work of teams. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures. Appreciates the wider business context, and how own role relates to other roles and to the business of the employer or client. | |
| **SFIA Professional Skill Level Description** | | |
| SCTY 3 | Communicates information security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to vulnerability assessments. Applies and maintains specific security controls as required by organisational policy and local risk assessments. Takes action to respond to security breaches in line with security policy and records the incidents and action taken. | |