**ATTACHMENT 1**

**STATEMENT OF WORK**

|  |  |
| --- | --- |
| **Nominated Candidate** |  |
| **Role** | ICT Security Specialist [Certifier] |
| **Contract Commencement Date** | On or after 1 October 2021 |
| **Contract Expiry Date** | 12 or 24 month contract terms will be considered  |
| **Purpose of Services:** | Professional Services (Clause 7.11) |
| **Role Description** | The ICT Security Specialist [Certifier] will be responsible under broad direction to protect ASD systems and information, meet domestic and international policies and standards, and mitigate risks. These responsibilities include carrying out SEA555 project certification activities. |
| **SFIA Level of Responsibility Required***Description Below* | The Specified Person will be expected to demonstrate attributes of SFIA Level of Responsibility 5 |
| **SFIA Skills Required***Description Below* | **INAS 5****SCTY 5****CORE 4****SCAD 3** |
| **Other Skills and Knowledge** | **Statement of Suitability Against Other Skills and Knowledge** |
| 1. Experience identifying and applying security controls to large scale, complex capabilities and/or developing ICT Security analytics (Essential)
 |  |
| 1. Experience architecting complex systems (Desirable)
 |  |
| 1. Experience in the provisioning of security controls to cloud computing systems (Desirable)
 |  |
| **Major Responsibilities:**  | **Statement of Suitability Against Major Responsibilities** |
| 1. Liaise with multiple project and capability stakeholders to assist in design and documentation of ICT system security controls
 |  |
| 1. Contribute to design of ICT Security policy and documentation, and implement practices, technologies and governance.
 |  |
| 1. Analyse and assess ICT system security documentation and configuration, including the use of vulnerability assessment tools.
 |  |
| 1. Undertake ICT security threat and risk assessments.
 |  |
| 1. Support the operation of the IT security team by providing the following services:

• IT security education and outreach• Professional leadership on IT security related matters and issues• Continuous improvement processes• Stakeholder engagement on security-related matters• Operational IT Security including device inspections and monitoring service desk queues |  |
| **Other Features of the Role (e.g. location, travelling, shift hours,)** | **Service Provider Response** |
| 1. Role will require some travel between ACT facilities
 |  |
| Prepared by: Sam IsbisterDate: 07 September 2021Authorised by: Mark Alexander |
| **SFIA Core Competencies** |
| **SFIA Level Of Responsibility 5**  |
| **Autonomy** | Works under broad direction. Work is often self-initiated. Is fully responsible for meeting allocated technical and/or project/supervisory objectives. Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities. |
| **Influence** | Influences organisation, customers, suppliers, partners and peers on the contribution of own specialism. Builds appropriate and effective business relationships. Makes decisions which impact the success of assigned work, i.e. results, deadlines and budget. Has significant influence over the allocation and management of resources appropriate to given assignments. |
| **Complexity** | Performs an extensive range and variety of complex technical and/or professional work activities. Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer/organisational requirements. |
| **Business skills** | Advises on the available standards, methods, tools and applications relevant to own specialism and can make appropriate choices from alternatives. Analyses, designs, plans, executes and evaluates work to time, cost and quality targets. Assesses and evaluates risk. Communicates effectively, both formally and informally. Demonstrates leadership. Facilitates collaboration between stakeholders who have diverse objectives. Takes all requirements into account when making proposals. Takes initiative to keep skills up to date. Mentors colleagues. Maintains an awareness of developments in the industry. Analyses requirements and advises on scope and options for continuous operational improvement. Demonstrates creativity, innovation and ethical thinking in applying solutions for the benefit of the customer/stakeholder. |
| **SFIA Professional Skill Level Description**  |
| **INAS 5** | Interprets information assurance and security policies and applies these in order to manage risks. Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines. Uses testing to support information assurance. Contributes to the development of policies, standards and guidelines. |
| **SCTY 5** | Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security, and recommends appropriate control improvements. Contributes to development of information security policy, standards and guidelines. |
| **CORE 4** | Conducts formal reviews of activities, processes, products or services. Collects, collates and examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences. Analyses evidence collated and drafts part or all of formal reports commenting on the conformance found to exist in the reviewed part of an information systems environment. |
| **SCAD 3** | Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard security administration tasks and resolves security administration issues. |