**ATTACHMENT 2**

**STATEMENT OF WORK**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nominated Candidate** | | |  |
| **Role** | | | Security Architect – Multiple positions |
| **Contract Commencement Date** | | | ASAP |
| **Contract Expiry Date** | | | Contract terms between 12 and 24 months will be considered |
| **Purpose of Services:** | | | Professional Services |
| **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 Architect.  The Security Architect will be accountable under broad direction to apply security and technical expertise to the design and documentation of tailored solutions. This includes development and communication of high-level security strategies and artefacts to influence the development of secure capabilities to meet challenging business needs in a complex operating environment. |
| **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* | | | **ARCH 5**  **SCTY 5** |
| **Other Skills and Knowledge** | | | **Statement of Suitability Against Other Skills and Knowledge** |
| 1. N/A | | |  |
| **Major Responsibilities:** | | | **Statement of Suitability Against Major Responsibilities** |
| 1. Actively engage with stakeholders to elicit security based requirements and communicate relevant progress of activities. | | |  |
| 1. Develop security architectures, both current, transitional and target state, based on organisational strategies and plans. | | |  |
| 1. Validate security requirements and traceability to solution designs and configurations. | | |  |
| 1. Develop architectural development of infrastructure technologies underpinning Enterprise ICT and analytic systems. | | |  |
| 1. Develop capability gap analysis based on the differences between the current and target state architectures and provide recommendations | | |  |
| 1. Ensure designs are appropriately aligned with organisational security standards and strategy; and that design activities and reviews canvass input from technical and security experts. | | |  |
| 1. Contribute to the approval of designs through architectural, security and stakeholder bodies. | | |  |
| 1. Provide leadership in the progression and resolution of security issues. | | |  |
| 1. Provide advice, guidance and assistance to less experienced colleagues as required. | | |  |
| 1. Work with project teams to ensure plans are updated as implementation evolves. | | |  |
| **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 Malone  Date: 15/12/2020  Authorised by: Travis 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** | | | |
| **ARCH 5** | Uses appropriate tools, including logical models of components and interfaces, to contribute to the development of systems architectures in specific business or functional areas. Produces detailed component specifications and translates these into detailed designs for implementation using selected products. Within a business change programme, assists in the preparation of technical plans and cooperates with business assurance and project staff to ensure that appropriate technical resources are made available. Provides advice on technical aspects of system development and integration (including requests for changes, deviations from specifications, etc.) and ensures that relevant technical strategies, policies, standards and practices (including security) are applied correctly. | | |
| **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. | | |