**ATTACHMENT 1**

**STATEMENT OF WORK**

|  |  |  |
| --- | --- | --- |
| **Nominated Candidate** | |  |
| **Role** | | System Security Architect/Practitioner for DEF103 Project |
| **Contract Commencement Date** | | ASAP |
| **Contract Expiry Date** | | 12 or 24 months after commencement date |
| **Purpose of Services:** | | Professional Services (Clause 7.11) |
| **Role Description** | | DEF103 is a major project to deliver Strategic Communications Capability to Defence.  The Project will undertake capital acquisitions to deliver new telecommunications capability services both domestically and internationally.  The System Security Architect/Practitioner is responsible for liaising closely with the Certification and Accreditation Authorities responsible for describing the security threats and risks with delivery of a solution.  The System Security Architect/Practitioner will develop the security architecture/design for the Project capabilities whilst working cohesively and adaptably with a large group of diverse stakeholders. |
| **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* | | SCTY 5  INAS 5  DESN 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. Determine security requirements by evaluating business strategies and leading threat risk assessment activities; research information security standards; conduct system security and vulnerability analyses and risk assessments. | |  |
| 1. Review existing system security measures, recommend and implement enhancements. | |  |
| 1. Expert knowledge of and ability to produce architectural solutions that meet the Australian Government Protective Security Policy Framework (PSPF and the Australian Government Information Security Manual (ISM). | |  |
| 1. Develop, deliver and update System Accreditation Plan (SAP), Security Risk Management Plan (SRMP) and other relevant documents to ensure Capability solution architecture/design(s) are able to sufficiently mitigate the identified threats. | |  |
| 1. Analyse, design, develop, deliver and maintain documentation supporting the security posture of a range of cyber security capabilities | |  |
| 1. Liaise with certification and accreditation authorities, business stakeholders and solution architects to drive a solution/design to an accreditation outcome. | |  |
| 1. Review internal/externally developed security engineering artefacts to ensure that all security requirements are addressed | |  |
| 1. Advise Program Design Authority on system security threats, risks and mitigations. | |  |
| **Other Features of the Role (e.g. location, travelling, shift hours,)** | | **Service Provider Response** |
| 1. The DEF103 Project will at times require Service Provider personnel to undertake domestic or international travel on behalf of the Commonwealth. | |  |
| Prepared by: Effie Belbin  Date: 23 November 2020  Authorised by: Doug Campbell | | |
| **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** | | |
| **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. | |
| **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. | |
| **DESN 5** | Specifies and designs large or complex systems. Selects appropriate design standards, methods and tools, consistent with agreed enterprise and solution architectures and ensures they are applied effectively. Reviews others’ systems designs to ensure selection of appropriate technology, efficient use of resources, and integration of multiple systems and technology. Contributes to policy for selection of architecture components. Evaluates and undertakes impact analysis on major design options and assesses and manages associated risks. Ensures that the system design balances functional, service quality, security and systems management requirements. | |