**3.8 Acquisition Security Support**

3.8.1 Security Manager

3.8.1.1 Specialized Experience and Education Requirements.

None, see Section 3.1.1

3.8.1.2 Minimally Required Tasks

3.8.1.2.1 The Contractor shall provide administrative, Acquisition Security, Personnel Security, Information Protection (IP), Anti-Terrorism/Force Protection (AT/FP), and Operations Security (OPSEC), COMSEC, Foreign Military Sales Security, support during the capabilities planning/pre-acquisition, acquisition, development, production and sustainment phases of various equipment and weapon systems within the framework of the defense acquisition management system. Tasks may include, but are not limited to, participation on IPTs and related activities, analyzing problems, defining alternative solutions, providing recommendations, writing reports, and accomplishing specifically assigned work as defined in individual tasks orders. The contractor shall conduct security site surveys for Enhanced End Use Monitoring (EEUM), which will require foreign travel and interaction with foreign customers.

3.8.1.2.2 The Contractor shall provide administrative, acquisition security, IP, antiterrorism/force protection, and OPSEC, COMSEC assistance during the capabilities planning/pre-acquisition, acquisition, development, production and sustainment phases of various equipment and weapon systems within the framework of the defense acquisition management system. Tasks may include, but are not limited to, participation on IPTs and related activities, analyzing problems, defining alternative solutions, providing recommendations, writing reports, and accomplishing specifically assigned work as defined in individual tasks orders. The Contractor shall conduct security site surveys for EEUM, which will require foreign travel and interaction with foreign customers.

3.8.1.2.3 The Contractor may not release or allow any foreign national access to U.S. Government information without direct approval from the U.S. Government. The Contractor may have access to another foreign government’s information at the unclassified and sensitive levels. The Contractor shall comply with the U.S. State Department's ITAR (22 Code of Federal Regulations [CFR] Parts 120-130 and Amendments), the Arms Export Control Act, Defense Trade Security Initiatives, State Department, USAF, and DoD policies relative to the ITAR and exporting and importing data especially for non-FMS cases. The Contractor and any subcontractors shall obtain a Technical Assistance Agreement (TAA) with each of the foreign nations identified by COR at the time of any resulting contract and for the duration of this contract within 120 days after notification with the appropriate agencies, such as the Department of State, to export and receive technical data to FAR Part 12/FAR Part 15 contract activities. The contractor shall maintain the TAA for the duration of the task order. Contractor personnel shall have no direct contact with foreign nationals until ITAR requirements are met.

3.8.2 Acquisition Protection Management

3.8.2.1 Specialized Experience and Education Requirements

None, see Section 3.1.1.

3.8.2.2 Minimally Required Tasks

3.8.2.2.1 The Contractor shall provide information protection oversight for all aspects of system protection, technology protection, and program protection planning as pertains to the Directorate’s programs. The Contractor shall assist in maintaining secure facilities and respond to alarms of the government facilities in accordance with Air Force requirements and directorate OIs. The Contractor shall assist in receiving and protecting classified information. The Contractor shall assist with conducting independent security studies and analyses as required with only general direction and guidance.

3.8.2.2.2 The Contractor shall assist the Chief of Security in ensuring program protection requirements are integrated into all program areas of this task as required by DoD, USAF, and Major Command (MAJCOM) policies. The Contractor shall assist with providing program protection guidance for the development of AT plans; provide information protection and industrial security support in efforts involving program protection IPTs, system security working groups, certification working groups, System Security Working Group, Certification Working Group, and IPTs; and provide acquisition security input for ICD, CDD, SOW, SOO, SRD, CONOPS, Security Test and Evaluation (ST&E), DID, CDRL, CDR, PDR, CCB, CCP, ECP, LCMP, SCG, Security Classification and Declassification Guides (SCDG), and DD Forms 254, Department of Defense Contract Security Classification Specifications.

3.8.2.2.3 The Contractor shall assist with preparing DD Forms 254 for signature, coordination and distribution by the appropriate government agency; maintaining status list and file maintenance of all contracts, solicitations and proposals for analysis and reports for the Chief of Security.

3.8.2.2.4 The Contractor shall assist in preparation of SCDGs for programs in which classified information is involved. The Contractor shall assist with ensuring classification, safeguarding and declassifying national security information determinations are made in conjunction with the program manager and technical staff of system/program involved. The Contractor shall provide the Government Chief of Security the classified Security Status Report. (CDRL A002)

3.8.3 Program Security Support

3.8.3.1 Specialized Experience and Education Requirements

None, see Section 3.1.1.

3.8.3.2 Minimally Required Tasks

3.8.3.2.1 The Contractor shall provide support to the Mobility and Presidential Support Directorates, as an advisor to senior program leaders and their management staff on information protection, program protection, personnel, and industrial security matters. The Contractor shall participate in security working groups and other meetings as required. The Contractor shall be responsible and accountable for compliance with applicable DoD, USAF, and AFMC security directives to include National Industrial Security Program Operating Manual (NISPOM), the NISPOM supplement and Joint Air Force-Army-Navy Manuals and Implementation Guide. The Contractor shall assist with developing and coordinating implementing security guidance for distribution to Government / industry team. The Contractor shall provide technical support and information protection, program protection, and industrial security guidance as it relates to acquisition security and developing countermeasures to negate vulnerabilities to actual and potential threat. The Contractor shall work in secure facilities, which will require performing end-of-day security checks and respond to alarms of the Government facilities in accordance with Air Force requirements and directorate OIs.

3.8.3.2.2 The Contractor shall assist with receiving classified materials and securing as appropriate. Because of this, the Contractor shall be accessed into some of the Government’s programs that are critical to national security. As such, this will require the Contractor to facilitate the implementation of these initiatives. The Contractor shall assist with checking information against security classification and declassification guide during the course of the Contractor information protection manager functions.

3.8.3.2.3 The Contractor shall assist with providing personnel security support to directorate programs. The Contractor shall provide information support and guidance concerning processing of investigative paperwork; document and validating background information for Government and Contractor members accessed to directorate programs to include reportable information; and providing personnel SA and guidance to technical and functional managers, clerical staff, and other program personnel.

3.8.3.2.4 The Contractor shall report program security incidents and violations and monitor security incident investigations. The Contractor shall prepare reports as identified on a case-by-case basis by the Program Security Officer (PSO).

3.8.3.2.5 The Contractor shall assist with preparing and processing Program Access Requests (PAR) for individuals requiring access to directorate programs. The Contractor will be trained, if required, of first tier review of PARs to ensure compliance with current DoD and SAF/AQ directives. The Contractor shall screen and verify all required forms and documentation to ensure they are complete and accurate before submitting to the PSO for signature; review each request received to determine validity for access indicated; conduct Defense Clearance and Investigations Index, Joint Personnel Adjudication System (JPAS), and local files checks; and accomplishing program indoctrination and maintaining list of approved and briefed personnel. The Contractor shall plan, manage, and administer the security education program to ensure material relative to special security programs is presented annually.

3.8.3.2.6 The Contractor shall provide accurate access information, via personnel security database or access rosters, for personnel attending conferences where program material is discussed.

3.8.3.2.7 The Contractor shall assist with executing the annual special security self inspection program; developing and updating required internal security processes and standard operating instructions relative to security and to ensure they are executed throughout the Directorate programs. The Contractor shall augment Contractor security inspections when requested by the Government.

3.8.3.2.8 The Contractor shall provide technical support to the Chief of Security for safeguarding classified information, mail, telephone inquiries, security-related questions, and incidents, and provide information in all areas of security requirements. The Contractor shall provide administrative support and assistance to the Chief of Security in accomplishing daily requirements, preparing analyses and reports, and recommending new and amended procedures.

3.8.3.2.9 The Contractor shall assist with maintaining the office file plan, in addition to computer-generated database records for the security manager.

3.8.3.2.10 The Contractor shall assist with accessing the Government-provided electronic messaging system on SIPRNet and monitoring the organization's mailbox regularly to ensure messages requiring action are promptly acted upon.

3.8.3.2.11 The Contractor shall escort personnel visiting the facility when required.

3.8.3.2.12 The Contractor shall assist with writing, co-developing, and staffing for approval with the associated country an EEUM security plan. The Contractor shall assist in the performance of security inspections and EEUM with Defense Security Cooperation Agency at various locations and countries outside the United States.

3.8.4 Security Administration Management

3.8.4.1 Specialized Experience and Education Requirements.

None, see Section 3.1.1.

3.8.4.2 Minimally Required Tasks

3.8.4.2.1 The Contractor shall assist with providing SA for all aspects of information, personnel, industrial, operations and communication security. The Contractor shall assist with performing a wide range of program security management activities, such as information, physical, operational, and personnel security. The Contractor shall assist with receiving classified materials, as required, in direct support of the WLE Security Office.

3.8.4.2.2 The Contractor shall assist with providing recommended courses of action after evaluating issues as they arise, and shall assist with preparing correspondence, briefing materials, and other documentation in support of the program office

3.8.4.2.3 The Contractor shall assist with communicating technical guidance as received from the Chief of Security to Government and Contractor personnel in areas of planning, implementation, and report progress in implementation of such directions; assisting with conducting studies and analyses as directed by the Chief of Security; and maintaining records for all personnel, both in-coming and out-going visits, in addition to maintaining an AIS database.

3.8.4.2.4 The Contractor shall assist with administratively process visit requests for security manager approval; coordinating visit requests with other program offices; and assisting the Chief of Security by in-processing new employees and preparing Entry Authorization Form (AF Form 2586).

3.8.4.2.5 The Contractor shall assist in the processing of each military, civilian, and Contractor individual assigned directorates into their organization through JPAS. The Contractor shall assist in tracking investigation/reinvestigation due dates. The Contractor shall assist in initiating and submitting an AF Form 2583. The Contractor shall assist with notifying individuals to contact the 88 ABW/IPP for an appointment for fingerprints. The Contractor shall assist with tracking the progress of the investigation through JPAS.

3.8.4.2.6 The Contractor shall assist the Operations Security Monitor in developing, maintaining and overseeing the OPSEC program. The Contractor shall assist in the establishment of an operations security working group to develop and implement an operations security plan.

3.8.4.2.7 The Contractor shall assist with the preparation of various documentation and charts for Government review and approval. The Contractor shall assist with preparing briefing documents, develop spreadsheets, databases, etc. to organize and store program data. The Contractor shall assist in retrieving data in the form of reports and queries. The Contractor shall be familiar with electronic media to distribute charts and documents to customers.

3.8.4.2.8 The Contractor shall assist in the planning, formulating, editing, developing, publishing, and distribution of finished products including but not limited to program documentation, reports, briefings, and other presentations (technical and non-technical, classified, and unclassified) in the media and format requested as required.

3.8.4.2.9 The Contractor shall assist with maintaining forms, files, and program reference libraries.

3.8.5 Information Systems Security Support

3.8.5.1 Specialized Experience and Education Requirements.

The Contractor shall demonstrate complete experience and expertise in the DoD’s information, industrial, operations, personnel, and communications security disciplines, within the framework of the defense acquisition management system and program protection planning, are required. Law enforcement and/or physical security expertise and experience are not substitutes for the indicated experience and expertise requirements. Successful completion of DoD’s Security Fundamentals Professional Certification or Industrial Security Oversight Certification is highly desired.

The Contractor shall possess one of the following IA certifications, IAW DoD 8570.01-M for IA work performance under this contract:

• A+ Computing Environment (CE)

• Network + CE

• Systems Security Certified Practitioner (SSCP)

• CompTIA Advanced Security Practitioner (CASP)

• Security + CE

3.8.5.2 Minimally Required Tasks. In addition to Section 3.8.1 and 3.8.2:

3.8.5.2.1 The Contractor shall provide technical assistance and support to the Mobility Directorate Security Office. The Contractor shall be responsible for maintenance and support of DoD and AF classified computing systems and networks to include cybersecurity, RMF, personnel processing for access to DoD Secure Internet Protocol Router Network (SIPRNet) and classified systems. Assistance will require individuals to obtain/maintain classified systems administrative privileges for SIPRNet and other systems. The Contractor shall perform system trusted downloads, burning classified CDs, maintain and update host system patches, implement mandated system vulnerability mitigations and set up user accesses and accounts. The Contractor shall be appointed as an Information Assurance Manager (IAM Level I) and IAT Level I requiring certification per DoD 8570.01-M. Personnel shall demonstrate proficiency in currently utilized Windows OS, Windows group policy objects, DoD cybersecurity, NIST RMF, STIGs, Endpoint Security System/ SS//HBS and DoD PKI.

3.8.5.2.2 The Contractor shall assist with implementation of DoD, USAF, and MAJCOM policies and develop local processes and procedures for the effective execution of the directorate security program. The Contractor shall assist with supporting technical implementation, maintenance, and oversight of the following elements of the directorate's Automated Data Processing (ADP) security program: certification, risk analysis, and operational support.

3.8.5.2.3 The Contractor shall assist with reviewing, analyzing, and developing full information for ADP system descriptions involving the establishment of new automated systems; determining the appropriateness of description detail, identify potential or actual system vulnerabilities, and recommend corrective action for higher authority approval/disapproval; and conducting in-depth technical analyses of ADP application and system software (including associated security related software) and equipment used by directorate security for the purpose of evaluating their effectiveness at meeting defined security requirements.

3.8.5.2.4 The Contractor shall assist with evaluating different versions of security software and installing security software.

3.8.5.2.5 The Contractor shall assist with interviewing operational personnel and reviewing documentation for the purpose of resolving technical security problems and issues, as a basis for drafting and recommending new policies, standards, procedures, and operating doctrines.

3.8.5.2.6 The Contractor shall assist with preparing system security plans for classified systems; accessing the Government-provided electronic messaging system on SIPRNet; and monitoring the organization's mailbox regularly to ensure messages requiring action are promptly acted upon.

3.8.5.2.7 The Contractor shall assist with monitoring information system activities to ensure system integrity. The Contractor shall assist with establishing reaction and maintenance control for the facility. The Contractor shall assist with performing system access or revocation tasks.

3.8.5.2.8 The Contractor shall assist with reporting system security incidents, classified message incidents, vulnerabilities, and virus attacks according to AFSSI 5021; and ensuring information systems are cleared or sanitized according to AFSSI 5020.

3.8.5.2.9 The Contractor shall assist in improving internal management processes by proposing and/or implementing improvements to visual, computer-based communications to manage critical processes.

3.8.5.2.10 The Contractor shall assist with managing and accounting for COMSEC equipment. The Contractor shall assist with receiving, accounting for, page checking, handling, using, and safeguarding all COMSEC material until it is destroyed or returned to the COMSEC account; and maintaining current operating instructions that cover handling, controlling, and protecting COMSEC assets, including inventory, two-person integrity (if applicable), destruction, and COMSEC incident reporting.

3.8.5.2.11 The Contractor shall assist in ensuring information security standards are maintained; opening, securing, and performing end-of day security checks; and responding to alarms IAW Air Force requirements. The Contractor shall assist in the planning, formulating, editing, developing, publishing, and distribution of finished products, including but not limited to program documentation, reports, briefings, and other presentations as required (technical and non-technical, classified, and unclassified) in the media and format requested. The Contractor shall assist with recommending courses of action after evaluating issues as they arise and prepare correspondence, briefing materials, and other documentation in support of the security office.

3.8.5.2.12 The Contractor shall assist with receiving from the Government Chief of Security to Government and Contractor personnel in areas of planning, implementation, and report progress in implementation of such directions; assist with conducting studies and analyses as directed by the Government Chief of Security; and receiving and storing classified materials, as required, in direct support of the WLE directorate security office