Contract #: GS06F0646Z
Task Order#: H92222-17-F-0199
Attachment 1
June 16, 2017

STATEMENT OF WORK

U.S. Army Special Operations Command (USASOC)

Application Management Support

1.0 DESCRIPTION OF SERVICES:

The objective of this task order is to provide Application Management (APM) Services for four USASOC Units; the USASOC G6, USASOC G6 Sensitive Activities (SA) Branch, and the 160th Special Operations Aviation Regiment (SOAR), and the U.S Army Special Operations Supply Support Activity (ARSOSSA).

2.0 PURPOSE:

Onsite support to develop, administer, and maintain portal, web, applications, and database development that span Non-Secure Internet Protocol Router Network (NIPRNET)/Secure Internet Protocol Router Network (SIPRNET)/ACCM /SAP classification levels in full accordance with Department of Defense (DoD) and organization regulations, directives, and customer procedures.

3.0 SPECIFIC REQUIREMENTS/DELIVERABLES

3.1 USASOC G6 Requirements:

The contractor shall provide portal, web, application, and database development and maintenance services in developing net centric applications to support functionally diverse business processes used in support of USASOC and its' subordinate units including their tactical operations. Support the development, migration, testing, documentation, integration, and maintenance of current and legacy applications, including Government Off-the-Shelf (GOTS) / Commercial Off-the-Shelf (COTS) products to support USASOC business needs for:

- Web-based software, applications and content
- Databases, database software, applications and content
- Application support for the development, migration, testing, documentation, integration, and maintenance of current and legacy GOTS/COTS software and new applications

3.1.1 Application Development and Support:

The contractor shall analyze requirements, design and code new software applications to support Government business processes, and provide application level support to engineering and configuration of Government acquired software. The Contractor shall develop all applications for use by HQ USASOC and components in a net centric environment. The Contractor shall perform the following tasks:

3.1.1.1 Provide a Software Development Plan (SDP) tailored specifically to address the work breakdown structure, detailed schedule with specific milestones, technical reviews and audits, software quality assurance, and status reporting for all software development efforts.

3.1.1.2 Provide a Version Description Document (VDD) to specifically address what core functionality and/or capability is being provided in a particular version of software application that is being delivered. Release notes will be provided for all hot fixes identifying new features, changes, fixed bugs and any additional known problems that are not otherwise addressed.

3.1.1.3 Provide a User Manual and comprehensive technical documentation for each new application. Additionally, the Contractor shall provide the policy and/or procedure underpinnings necessary for the government to publish official documents that dictate processes, procedures, and security requirements associated with each development effort.

3.1.1.4 Provide assistance to the government by training staff on the use of developed software to include the preparation of training materials, delivering the User Manual, demonstrating the application, providing sample test data and preparing scripts to support training objectives.

3.1.1.5 Assist the Integration & Test Lab (ITL) by evaluating custom 3rd party ASP.Net products. Assist the ITL by evaluating custom software, producing software engineering reports and application design reviews. Determine 3rd party applications integration and deployment for use on SOFNet/XNET/SAP.

3.1.1.6 Ensure standard features are leveraged when possible including navigation controls, user management, and following any Look and Feel policies produced by USASOC.

3.1.1.7 Conduct technology and product research on solutions and configurations, Active Directory authentication, MS Virtual Server, SMTP server implementation, and other technologies that have become standard tools.

3.1.1.8 Ensure the development environment matches the production environment as closely as possible by modifying the configuration when necessary.

3.1.1.9 Ensure the pre-release environment and/or staging environment matches the production environment as closely as possible to host applications for users Operational Testing and Evaluation (OT&E).

3.1.1.10 Use SharePoint as the presentation level for all applications where possible.

3.1.2 Web Development and Support:
The Contractor shall provide support for the development, migration, testing,

documentation, integration, and maintenance of GOTS/COTS web-based software, applications, and content in accordance with applicable DOD and USASOC regulations.

3.1.3 Database Development and Support:
The Contractor shall provide support for the development, migration, testing, documentation, integration, and maintenance of current and legacy GOTS/COTS databases, database software, applications, and content in accordance with applicable DOD regulations. The following paragraphs define the database development and support to be provided:

3.1.3.1 Develop, migrate, test, document, integrate, and maintain databases, applications, stored procedures, and associated reports and forms.

3.1.3.2 Provide consulting services on database development and integration issues.

3.1.3.3 Assist in development of metadata standards and reference tables for USASOC DBs.

3.1.3.4 Ensure that SharePoint is utilized as the presentation layer for all development efforts where possible to include using page viewer web parts to display data.

3.1.4 Data Warehouse Support:
The Contractor shall provide dedicated web, application, and DB support services in developing a centrally managed warehouse of functionally diverse data in support of the USASOC Data Warehouse. This data warehouse will be used USASOC-wide to capture and feed datamarts. Specific requirements include:

3.1.4.1 Capture both classified and unclassified data on balanced scorecard measures from their organic DBs or create a method of data entry for SOF unique data.

3.1.4.2 Develop DB to be accessible in read and/or write capability by USASOC, its higher headquarters and CSC/CSU's.

3.1.4.3 Data captured will be from an Authoritative Data Source (ADS) designed to be retrieved, used and archived over an indefinite period of time.

3.1.4.4 All Software applications and database data elements shall adhere to existing DoD Data standards ensuring logical data models are fully attributed, normalized, and included in a data dictionary. The data dictionary will include the following information for each functional data element: the logical data element name, its definition that describes the meaning and the context of the data element in the system, the domain of the data element (the allowable values), the data type, length and unit of measure. All meta tags, where applicable, will be documented in an XML Schema (XSD file) and posted to the Metadata Registry after approval by CIO G6 Government personnel.

3.1.4.5 Ensure the lessons learned from other USASOC development efforts are applied across all new software applications ensuring data standards are validated against the DoD Metadata Registry (MDR), maintained, documented and reused to the maximum extent possible.

3.1.4.6 Assist in the development of effective disaster recovery solutions to ensure continuous access to critical data supporting the USASOC footprint.

3.1.4.7 Ensure that data is protected for privacy and security in compliance with applicable policies and regulations.

3.1.4.8 Provide documentation to Information Assurance to support the development of the System Security Authorization Agreement (SSAA) documentation and support Security Plan development, implementation, and maintenance.

3.1.4.9 Perform Technical and Cross functional review of data ensuring software applications and databases developed are capable and flexible to import and export applicable standardized data from external authoritative sources directly or through standardized interfaces, front-end or back-end translators or utilities.

3.1.4.10 Develop historical views and archiving solutions to meet USASOC directed recordkeeping standards and functional user business rules.

3.1.4.11 Technical Data and Computer Software Rights: TBD.

3.1.5 Maintenance of Current and Legacy Applications:
The Contractor shall provide development, migration, testing, documentation, integration, and maintenance of current and legacy GOTS/COTS software and applications in accordance with applicable DoD regulations. The Contractor shall:

3.1.5.1 Develop, migrate, test, document, integrate, and maintain software and applications.

3.1.5.2 Provide consulting services to users on application and software development.

3.1.5.3 Provide maintenance and connectivity to all required legacy systems and applications.

3.1.5.4 Redesign and recode the base applications as the production network configuration is modified.

3.1.5.5 Update and provide software development plans, version description documents, user manuals and technical documentation as required.

3.1.5.6 Evaluate applications to determine if they can be replaced or consolidated with newer technologies that are more in-line with USASOC standardization efforts.

3.1.6 Implementation for Security Controls for Software Application Development Efforts:

3.1.6.1 The developer shall provide information regarding their system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes.

3.1.6.2 The developer shall ensure adherence to secure coding practices identified in the Defense Information Systems Agency (DISA) Security Technical Implementation Guidance (STIG) Application and Security Development STIG as well as guidance in other relevant STIGs.

3.1.6.3 The developer shall deliver the software application, system, component, or service with security configurations consistent with DoDI 8510.01 and DISA STIGs/Security Requirement Guides (SRGs).

3.1.6.4 The developer shall use the applicable requirements from DoDI 8510.01 and STIGs/SRGs as the default for any subsequent system, component, or service reinstallation or upgrade.

3.1.6.5 The developer shall identify early in the system/software development life cycle, the functions, ports, protocols, and services intended for use with the software application and ensure the software development and maintenance effort address compliance with DoDI 8551.01 Ports, Protocols, and Services Management (PPSM).

3.1.6.6 The developer shall provide design information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code, and the RMF defined design/information.

3.1.6.7 The developer shall demonstrate the use of a system software development life cycle that includes Army and DoD state-of-the-practice system/security engineering methods, software development methods, testing/evaluation /validation techniques, and quality control processes consistent with AR 70-1, Research, Development, and Acquisition, Army Acquisition Policy and DoD Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System.

3.1.7 Support for Developed Software Applications:

3.1.7.1 The contractor shall sustain and maintain the following software applications currently in-place, automated and networked, the contractor shall sustain and maintain

SWCS's in-place, automated and networked, holistic individual assessment system on the SOFTNet network for the identified modules: configurations require sustained and periodic software maintenance

3.1.7.2 Applications:

- SWC Tracking of Administrative Record System (STARS)
- G4 Non-Tactical Vehicles
- ARSOAC Cub/Stripes
- Required Capability Analysis (RCA)
- RMA
- HICAT
- MDMS
- SharePoint Random Number Generator
- SharePoint Export to Word
- DTT/TMT
- ATLAS

3.1.8 Customer Support:

3.1.8.1 The Contractor shall provide elevated Tier technical support for the users of all developed applications. The Contractor shall coordinate resolution of elevated trouble tickets and when required submit escalated functional problems. Where possible, the assigned personnel will create Help information available on the SharePoint portal for USASOC users and Tier I/2 personnel to use – the objective being to reduce the number of elevated trouble tickets.

3.1.9 Training Support: The Contractor shall provide classroom, desk-side instruction, and self-paced web based training for all functional in-house developed applications.

3.1.10 Portal Support:
Consists of developing, testing, documenting, integrating and maintaining current and future portal application technologies.

3.1.10.1 Provide engineering recommendations for replicating SharePoint portal applications across the USASOC footprint. Ensure solutions meet DISA regulations and USASOC requirements for security.

3.1.10.2 Provide Disaster Recovery recommendations in support of SharePoint portal applications across the USASOC footprint.

3.1.10.3 Provide High Availability recommendations for SharePoint portals across the USASOC footprint.

3.1.10.4 Provide guidance and assistance to the Tier II web and database team for architecture and Best Business Practices.

3.1.10.5 Perform portal migrations to the latest technology as directed by USASOC G6.

3.1.10.6 Perform portal feature development IAW published Best Business Practices to fulfill user requirements.

3.1.10.7 Ensure all developed products do not interfere with the integrity of the SharePoint farms.

3.1.10.8 Ensure all developed products do not contain any classified data so they can be shared with the larger DoD development community.

3.1.10.9 Ensure all developed products meet IA and USASOC policies regarding security and PII.

3.1.10.10 Participate and publish documentation and developed products in the DoD's Source Forge website: https://www.forge.mil/

3.1.11 Schedule and Work Management

3.1.11.1 The contractor shall implement a project control system that will assist in effective management of all schedule and work elements of the program. This system must provide accurate and rapid insight into the contractor's milestones, performance, areas of difficulty and their impact, and schedule adjustment. The Contractor shall maintain a control system for scheduling, authorizing work, and tracking milestones.

3.1.11.2 The contractor shall prepare and submit a written Project Management Plan (PMP) (CDRL A001). The PMP shall list deliverables, proof of concepts, prototypes, events, working groups, meetings, and key milestone events. It shall also include a comprehensive calendar that lists the due date for project reviews, technical progress reports and monthly fiscal reports, Work Breakdown Structure (WBS), project overview, background, objectives, identification of the customer with POC information and contract point of contact information, description of the contract vehicle, period of performance, contract value, and description of facilities, equipment, and materials required to execute all contractual tasks. The contractor shall adhere to the PMP as proposed. The Contractor shall include updates to the Project Schedule and WBS in the Monthly Status Reports.

3.2 USASOC G6 SA Branch Requirements:

3.2.1 The contractor shall provide planning, engineering and testing a web portal and database intensive applications into an existing architecture. Beyond the initial operating capabilities, plans should also include scaling for expansion, redundancy and distributed

processing at remote sites. Personnel assigned to this Branch requires Focal Point and Special Access Program (SAP) clearances. This task applies primarily to the USASOC Fort Bragg location but will involve support at other CONUS locations. Below are some of the current and planned applications:

3.2.2 Applications:

- ACCM E-mail/Web Portal – Share Point
- Secured Property Book Unit Supply-Enhanced (S-PBUSE)/SAP PBUSE – Oracle
- Ordnance Management System (OMS) – Backend SQL
- Procurement Defense Desktop (PD2) – Oracle
- Automated message Handling System (AMHS) –SQL
- ATLAS (Requirements gathering & work will be conducted at ARSOSSA HQs)
- SCILS
- DTT/TMT

3.2.3 Web Development and Support:
The Contractor shall provide support for the development, migration, testing, documentation, integration, and maintenance of GOTS/COTS web-based software, applications, and content in accordance with applicable DoD and USASOC regulations.

3.2.4 Database development, integration, and testing:
Performs duties to include engineering the architecture, planning installation and integration, testing and documentation of database systems for which new applications are being planned and incorporated.

3.2.5 Position Requirements:

- Database Administrator (TS/SCI, SAP, ACCM)
- Business Systems Analyst (TS/SCI, SAP, ACCM)
- Portal Admin (TS/SCI, SAP, ACCM)

3.2.6 Web Development requirements

3.2.6.1 The Contractor shall support Full Cycle Portal/web development and implementation. Must have strong experience in Windows Share Point Service and Microsoft Share Point Server, JAVA, Info Path services, Portal/web security and using DOC AVE application. Ability to plan and implement portal solutions. Provide logical portal security management and maintain logical portal on a daily basis to ensure continuous operations to supported users.

3.2.7 Additional requirements:

3.2.7.1 The contractor shall have strong customer relationship skills. Ability to write and present reports. Knowledge of United States Army Special Operations. Logistical process knowledge is a plus.

3.3 160th SOAR Requirements:

The contractor shall provide development, administration, and maintenance for Microsoft Office SharePoint Services (MOSS) Portal and SQL Databases.

3.3.1 Microsoft Office SharePoint Portal Development and Maintenance:

The contractor shall develop, administer, and maintain Microsoft Office SharePoint Portals that span NIPRNET/SIPRNET/ACCM classification levels in full accordance with DoD and organizational regulations, directives, and procedures. The contractor shall identify existing SharePoint documentation, review those documents for understanding and completeness, and make recommendations for updating the documents. The technical and functional requirements will be defined and documented in accordance with the organizational policies, regulations, and directives. Required DoDAF artifacts will be specified in the 160th Special Operations Aviation Regiment (SOAR) design; however, at a minimum, the contractor shall develop and maintain a SharePoint Requirements Traceability Matrix (RTM). Once the baseline documents are established, the contractor shall maintain configuration control and evolve per DoD, USSOCOM, USASOC and Regimental regulations, directives, and procedures. The contractor shall manage users, monitor permissions, create/delete sub-sites, maintain backups, and perform other tasks related to operating and maintaining the SharePoint capability across the 160th SOAR (A).

3.3.1.1 Web Development and Search Optimization Strategy

The contractor shall plan the overall strategy regarding web development and search optimization. The contractor shall design the collaboration sites utilizing the most current SOCOM approved Microsoft Office SharePoint Server (MOSS) version for 160th SOAR (A) capabilities, facilitating collaboration throughout the various mission activities supported by the 160th SOAR (A). The contractor shall use the most current SOCOM approved Web technologies to optimize the search capabilities within MOSS while also complying with DoD, USSOCOM, USASOC, and Regimental regulations, directives, and procedures. The contractor shall evaluate and assess immerging/new technologies for potential migration and integration into the current architecture and capabilities. In addition, the contractor shall develop custom web interfaces to leverage the full capabilities of the search optimization solution.

3.3.1.2 Web and Portal Policy, Procedure, and Standard Formulation

The contractor shall formulate policies, procedures, and standards relating to web and portal administration and monitor system performance. The contractor shall ensure policies, procedures, and standards are compliant with DoD Directives 5210.2, 8000.1, 8320.02, 8500.01E, and other guidance related to webs and portals. The contractor shall implement and enforce compliance with the appropriate web and portal policies and procedures in the operations and maintenance of the SharePoint capabilities. In addition, the contractor shall identify vulnerabilities and gaps in the existing policies and procedures, and make appropriate recommendations to improve the overall operation and

security of the MOSS implementation.

3.3.1.3 SharePoint Medium Server Farms and Web Servers

The contractor shall support the Data Center Provider with research, design, test, install, troubleshoot, and Tier III support for the regiment's MOSS architecture. The contractor shall configure the architecture of the SharePoint server infrastructure for optimal efficiency, balancing operational requirements with technical and resource constraints, to provide robust capabilities to the 160th SOAR (A). Server farms will be grouped with like activities. The contractor shall ensure front-end servers are used for processing web pages, and other services (e.g., searching, spreadsheets, storage, and other database activities) are processed using the back-end server. The contractor shall research and use the latest software development methodologies and processes in conjunction with SharePoint capabilities. The SharePoint and web servers shall be operated and maintained using the current Security Technical Implementation Guides (STIG). The contractor shall back up the servers, monitor databases, fix corrupt databases, monitor communications, monitor memory, monitor server load, monitor server performance, and perform other operations and maintenance tasks to ensure optimal operations per established 160th SOAR (A) procedures and maintenance schedules.

3.3.1.4 Documentation Development

The contractor shall author documentation such as system specifications, technical analyses, design plans, implementation plans, and build documents. The contractor shall follow the System Development Life Cycle (SDLC) processes and methodologies, such as International Organization for Standardization (ISO) 12207 or Capability Maturity Model Integration (CMMI), to document development projects. This includes documentation of requirements, technical design, coding, testing, and implementation activities. The contractor shall prepare and update specific SDLC-related documents, such as the following:

- Requirements Traceability Matrix (RTM)
- System Requirements Specification (SRS)
- System Architecture Design (SAD)
- System Design Document (SDD)
- System Test Plan (STP)
- Version Description Document (VDD)
- Installation and Configuration Guide
- Operations and Maintenance Guide

3.3.1.5 Continuity of Operations (COOP) Planning and Testing

The contractor shall support the Data Center Provider with the planning, implementation, and testing of COOP strategies, backup, and recovery procedures of web systems and portals. The contractor shall follow COOP guidance established per DoD Directive 3020.26 and Army Regulation (AR) 500-3. The contractor shall perform COOP planning and testing across network/security domains and capabilities for hardware (HW) and software (SW).

The system will be managed as mission critical, with some Critical-Sensitive Positions, per 160th SOAR (A), Army, and USSOCOM Continuity of Operations Program Policy and Planning. The contractor shall work collaboratively with 160th SOAR (A) stakeholders to proactively understand requirements and document COOP processes to ensure a thorough and complete support of systems, including responsibilities, without adversely impacting the end users' day-to-day operations. The contractor shall examine the necessary HW and SW requirements to ensure business and operational continuity of 160th SOAR (A) systems and work with the Government to establish redundant capabilities. Additionally, the contractor shall pre-position critical emergency files on external backup servers. The contractor shall test the COOP plan at least annually or based on the duration set by the 160th SOAR (A).

3.3.1.6 DoD Information System Security

The contractor shall ensure compliance with DoD Information System Security policies, functionality, and optimization. The contractor shall operate and maintain secure systems per 160th SOAR (A) Information System Security policies and DoD Directives 8500.01E and 8570.01. Specifically, Information Assurance requirements shall be identified and included in the acquisition, design, installation, operation, upgrade, or replacement of all components of the system. The contractor shall maintain the system at an appropriate level of confidentiality, integrity, authentication, nonrepudiation, and availability that reflects a balance among the importance and sensitivity of the information, documented threats and vulnerabilities, the trustworthiness of users and interconnected systems, the impact of impairment or destruction to the system, and cost effectiveness. The contractor shall apply system patches per Information Assurance Vulnerability Alerts (IAVA). In addition, the contractor shall manage vulnerabilities and risks through the DoD Information Assurance Certification and Accreditation Process (DIACAP). The contractor shall prepare and provide appropriate DIACAP documents and implement improved security procedures based on scanning and audit results.

3.3.1.7 Relational Database System Design and Development

The contractor shall aid in the design and development of relational database systems and their web interfaces. The contractor shall use an iterative approach, such as Agile Development Methodology, to deliver incremental capabilities in response to user requirements. Also, the contractor shall use an SQL relational database management system (RDBMS) to design and develop a collaborative system with corresponding web interfaces. The contractor shall design and develop using programming languages such as .Net, JavaScript, DHTML, Silverlight, and other emerging technologies to dynamically search and display data and information. Web interfaces shall be Section 508 compliant and meet industry standards for usability, visualization, functionality, and accessibility. The contractor shall integrate these web interfaces into the SharePoint platform to enable access to the back-end database.

3.3.1.8 Virtual or Physical Test Systems

The contractor shall create and administer virtual or physical test systems and coordinate tasks with the System Administration team. The contractor shall create and administer testing activities in conjunction with the System Administration team and per DoD, USSOCOM, USASOC, and Regimental regulations, directives, and procedures. The contractor shall create and utilize a test database for loading test plans and test cases and for monitoring testing, bug fixes, and status. The contractor shall use the RTM to ensure test plans and use cases cover all the documented requirements. The contractor shall conduct load testing using automated testing software such as load runner software or a macro to simulate simultaneous users. The contractor shall evaluate the results and share the results with the 160th SOAR (A), making recommendations for improvements. The contractor shall document test results, fix bugs, conduct regression testing, track open issues, and schedule items to be fixed in future releases. The contractor shall coordinate systems changes with IT support contractors and systems administrators from interconnected systems to ensure there are no larger operational system impacts.

3.3.1.9 Web Server and Site Performance

The contractor shall monitor web server and site technical performance. The contractor shall monitor site performance, including web server and technical performance, per DoD, USSOCOM, USASOC, and Regimental regulations, directives, and procedures. The contractor shall recommend and use approved web services monitoring tools to monitor the availability, performance, stress, reliability, scalability, and integrity of the web services, such as Microsoft Performance Monitor.

3.3.1.10 Infrastructure Planning, Integration, and Disaster Recovery

The contractor shall assist the Data Center Provider (as applicable) with the infrastructure planning, integration, and disaster recovery support for web and portal servers and services at Fort Campbell, Hunter Army Air Field (AAF), and Joint Base Lewis-McChord that span NIPRNET/SIPRNET/ACCM classification levels in full accordance with DoD, USSOCOM, USASOC, and Regimental regulations, directives, and procedures. The contractor shall work with the Information Technology Management Office (ITMO) and local installation IT organization to identify Enterprise IT planning considerations for NIPR, SIPR, and ACCM networks. The contractor shall create network diagrams and identify necessary HW and SW requirements for redundant capability and create a procedures guide for implementation in the event the COOP must be executed. The contractor shall perform the following activities per DoD Directive 8500.01E, DoD Directive 3020.26, and AR 500-3:

- Infrastructure planning at Fort Campbell, Hunter AAF, and Joint Base Lewis-McChord that span NIPRNET/SIPRNET/ACCM classification levels
- Integration at Fort Campbell, Hunter AAF, and Joint Base Lewis-McChord that span NIPRNET/SIPRNET/ACCM classification levels
- Disaster Recovery support for web and portal servers and services at Fort Campbell, Hunter AAF, and Joint Base Lewis-McChord that span NIPRNET/SIPRNET/ACCM classification levels

3.3.2 Microsoft SQL Databases

The contractor shall develop and maintain Microsoft SQL Databases that span NIPRNET/SIPRNET/ACCM classification levels in full accordance with DoD and organization regulations, directives, and customer procedures. The contractor shall develop and maintain the Microsoft SQL Databases. The contractor shall design, document, test, implement, and maintain the database structure based on 160th SOAR (A) needs and requirements and will span the NIPRNET, SIPRNET, and ACCM classification levels. The contractor shall ensure the database architecture includes logical and physical infrastructure across the NIPRNET, SIPRNET, and ACCM classification levels. The technical and functional requirements will be defined and documented; an RTM will be provided, and the current baseline architecture will be documented using the DoDAF Framework.

3.3.2.1 Database Development and Optimization Strategy

The contractor shall plan the overall strategy regarding database development and optimization for the Microsoft SQL Databases for 160th SOAR (A) capabilities, facilitating collaboration throughout the various analysis activities required for development. The contractor shall assess the latest available technologies and make recommendations to optimize the search capabilities within the SQL Database infrastructure. The contractor shall use the provided tools to monitor database performance and implement load-balancing techniques to optimize performance. Also, the contractor shall implement clustering technologies and database design techniques to meet availability standards as defined by the 160th SOAR (A).

3.3.2.2 Database Policy, Procedure, and Standard Formulation

The contractor shall formulate policies, procedures, and standards relating to database management. The contractor shall document policies, procedures, and standards for shared, relational databases per DoD Directive 8320.02, Army Regulations, and USSOCOM/USASOC/160th SOAR (A) policies and procedures. The contractor shall manage the database using the approved governance structures, taxonomies, maintenance plans, ER-Diagrams, and other policy guidance.

3.3.2.3 Transaction Activity and Utilization Monitoring

The contractor shall monitor transaction activity and utilization and conduct performance tuning of indexes and databases. The contractor shall maintain a log of database transaction activity on the server to support debugging and short-term analysis of usage. The contractor shall purge or overwrite transaction logs as database backups are taken that supersede them. The contractor shall monitor logs weekly to determine capacity issues that result from high server utilization. If necessary, the contractor shall perform corrective actions, such as index optimization and increasing server resources.

3.3.2.4 SQL Server Farm Tier III Support

The contractor shall research, design, test, install, troubleshoot, and provide Tier III support for multiple SQL Server Farms and instances. The contractor shall establish

baseline configuration and make recommendations for improving the 160th SQL solution using clustering, mirroring, and other best practice techniques. The contractor shall configure the SQL server infrastructure for optimal efficiency. The contractor shall group server farms with like activities. The contractor shall back up the servers, monitor databases, fix corrupt databases, monitor communications, monitor memory, monitor server load, monitor server performance, and perform other operations and maintenance tasks to ensure optimal operations. The contractor shall provide Tier III support for SQL servers per 160th SOAR (A) service desk policies and procedures.

3.3.2.5 Documentation Development

The contractor shall author documentation such as system specifications, technical analyses, design plans, implementation plans, and build documents. The contractor shall document data definitions, physical data models, logical data models, and enterprise data models and shall develop or update baseline database documents using standard approaches, methodologies, and frameworks such as CMMI and DoDAF.

3.3.2.6 COOP Planning and Testing

The contractor shall plan, implement, and test COOP strategy, backup, and recovery procedures of database systems. The contractor shall follow COOP guidance established per DoD Directive 3020.26 and AR 500-3. The contractor shall perform COOP planning and testing across network/security domains and capabilities for both hardware and software. The system shall be managed as mission critical, with some Critical-Sensitive Positions, per 160th SOAR (A), Army, and USSOCOM Continuity of Operations Program Policy and Planning. The contractor shall work collaboratively with 160th SOAR (A) stakeholders to proactively understand requirements and document COOP processes to ensure a thorough and complete support of systems, including responsibilities without adversely impacting the end users' day-to-day operations. The contractor shall examine the necessary HW and SW requirements to ensure business and operational continuity of 160th systems and work with the Government to establish redundant capabilities. The contractor shall pre-position critical emergency files on external backup servers. Also, the contractor shall test the COOP plan at least annually, or as directed.

3.3.2.7 Database Design and Integration Review

The contractor shall review database design and integration of systems and make recommendations regarding enhancements and/or improvements. The contractor shall review current database design and architecture of the various interrelated systems and make recommendations based on industry best practices for designing, engineering, and implementing shared relational databases. The contractor shall progressively assemble a detailed description of critical enterprise warfighting and business processes mapped to system functions and data. The contractor shall work closely with users, developers, and the 160th SOAR (A) to ensure that any existing operational concepts, requirements, use cases, data tables, or other documentation are reviewed, understood, and incorporated as part of the baseline data model. The contractor shall analyze stakeholder needs and

requirements, operational functions and processes, system interfaces and characteristics, and the enterprise architecture to decompose the 160th SOAR (A)'s mission into individual data elements, and then design an integrated database solution that links the mission, functions, roles, and responsibilities of the 160th SOAR (A) across the Enterprise.

3.3.2.8 Stored Procedures Development

The contractor shall develop stored procedures and/or triggers. The contractor shall document, develop, test, and implement procedures to prevent unauthorized access to stored data on the 160th SOAR (A) database architecture infrastructure. The procedures shall include integration of various procedures related to personnel security, information security, information assurance, systems security, and other measures to ensure the confidentiality, integrity, and availability of data are maintained across the enterprise. The contractor shall include step-by-step procedures on processing, storing, and disseminating stored information to authorized users. In addition, the contractor shall develop procedures for auditing and enforcing compliance with stored policies and submit them for approval to the 160th SOAR (A).

4.0 SECURITY REQUIREMENTS

4.1 The contractor shall support security accordance with the attached DD254. Contractor team individual(s) supporting this task will be cleared at the Secret levels at the start of this task. Contractors will require access to NIPRNET/SIPRNET/ACCM.

4.2 The contractor shall ensure requirements for safeguarding classified information and classified materials, for obtaining and verifying personnel security clearances, for verifying security clearances and indoctrination of visitors, for controlling access to restricted areas, for protecting government property, and that the security of automated and non-automated management information systems and data is fulfilled. The contractor's management system shall prevent unauthorized disclosure of classified and sensitive unclassified information. The Government shall be immediately notified of any security incident or any indication of a potential unauthorized disclosure or compromise of classified or sensitive unclassified information.

4.3 The contractor shall provide security management support. Typical efforts include, but are not limited to, performing classified document control functions, classified materials inventories, program access requests, preparing and monitoring personnel indoctrination and debriefing agreements, and maintaining and using security related databases.

4.4 AT Level I training. All contractor employees, including subcontractor employees, requiring access to an Army or USSOCOM controlled installation, facility, or area shall

complete AT Level I Awareness Training within 60 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever applies. The contractor shall submit certificates of completion for each affected contract employee and subcontract employee to the COR (or to the contracting officer, if a COR is not assigned) within 90 calendar days after completion of the training by all employees and subcontractor personnel. This is an annual training requirement. AT Level I training is available at: https://jkodirect.jten.mil/Atlas2/faces/page/login/Login.seam.

4.5 Access and general protection policy and procedures. All contractor employees, including subcontractor employees, requiring access to an Army or USSOCOM controlled installation, facility, or area shall comply with applicable security policies and procedures (provided by the government representative). This includes policies pertaining to the use or prohibition of electronic recorders, devices, cameras, etc. If the Contractor is required to take photographs or videos on a Government Installation, the Contractor must obtain written permission from the Senior Commander. The contractor shall also provide all information required for background checks to meet installation and facility access requirements to be completed by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. The contractor workforce must comply with all personal identity verification requirements as directed by DoD, HQDA, USSOCOM, USASOC and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should Force Protection Condition (FPCON) at any individual facility or installation change, the government may require changes in contractor security matters or processes.

4.6 For contractors requiring Common Access Card (CAC). Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

4.7 For contractors to maintain and recover a CAC. Contractor shall comply with DoDI 5200.46, dated 9 Sep 14, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC). When eligibility is denied, revoked, contract completion, or contractor fails to maintain the DODI Basic Adjudication Standards or Supplemental Adjudication Standards listed within, CACs will be recovered by the Contractor and will immediately be rendered inoperable and returned to the COR or the local Real-time Automated Personnel Identification System (RAPIDS) site and the turn-in receipt forwarded to the COR. In addition, agencies' physical and logical access systems will be

immediately updated to eliminate the use of a CAC for access. Contractor shall report departed employees and the dates their CAC were returned to the COR or RAPIDS site as of the last day of the month on a monthly basis IAW SOFARS clause 5652.242-9002. The report will include the names and circumstances of those departed employees whose CAC was not retrieved. Negative reports are required.

4.8 iWATCH training. The Vendor and all associated sub contractors shall brief all employees on the local iWATCH program (training standards provided by the government requiring activity Antiterrorism Officer (ATO)). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR or the designated security office. Training shall be completed within 60 calendar days of contract award and within 30 calendar days of new employees' commencing performance with the results reported to the COR no later than 90 days after contract award and new employees' commencing performance.

4.9 Access to government information systems. All contract employees with access to a government information system must be registered in the Army Training Certification Tracking System (ATCTS) at commencement of services and must successfully complete the DoD Information Assurance Awareness training prior to access to the information system and then annually thereafter.

4.10 Requirement for OPSEC training. Per AR 530-1, Operations Security, new contract employees must complete OPSEC Level I training within 30 calendar days of reporting for duty. All contract employees must complete annual OPSEC Awareness Training.

4.11 Information assurance/information technology training. All contractor employees and associated subcontractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD, Army, USSOCOM and USASOC training requirements in DODD 8570.01, DoD 8570.01-M, AR 25-2 and published USSOCOM and USASOC requirements within 180 calendar days of employment.

4.12 Information assurance/information technology training certification. Per DoD 8570.01-M, DFARS 252.239.7001, and AR 25-2 the contractor employees' supporting IA/IT functions shall be appropriately certified upon contract award. Baseline certification as stipulated in DoD 8570.01-M, must be completed upon contract award.

4.13 Handling / access to classified information. The Vendor shall comply with *FAR 52.204-2, Security Requirements* for access to information classified "Confidential", "Secret", or "Top Secret". The Vendor must execute a Security agreement (DD Form 441), IAW the National Industrial Security Program Operating Manual (DoD 5220.22-M) and any revisions to DoD 5220.22-M (Note: A DD Form 254 will be required for any contract that requires access to classified information and/or a security clearance.)

4.14 Vendor to obtain a Facility Clearance and individual clearances at the appropriate level. The Vendor must obtain a Facility Clearance at the appropriate level (IAW the NISPOM DoD 5220.22-M) prior to the start of the contract awarded period of performance. Contractor personnel performing work under this contract must have the required security clearance at the appropriate level at the start of the period of performance. Security clearances and Facility Clearance (FCL) requirements are required to be maintained for the life of the contract in accordance with the DD254 attached to the contract.

4.15 Pre-screen applicants using E-Verify Program. The Vendor must pre-screen applicants using the E-verify Program (http://www.dhs.gov/E-Verify) website to meet the established employment eligibility requirements. The vendor must ensure that the applicant has two valid forms of government issued identification.

5.0 REPORTS. CDRLs 1 – 21 will apply to this task order.

- Transition-In Plan (30 Days after Award)
- Quality Assurance Plan (30 Days after Award)
- Monthly Contractor Status Report (Monthly)
- Standard Operating Procedures (As Rqd)
- Services & Procedures Recommendations (As Rqd)
- Project Status Reports (As Rqd)
- In-Progress Reviews (As Rqd)
- Software Development Plan (As Rqd)
- Version Description Document (VDD) (Rqd)
- User manual (As Rqd)
- Detailed installation guide (As Rqd)
- Accreditation documentation (As Rqd)
- Exit Plan (60 Days prior to Contract Termination)

6.0 Quality Assurance Surveillance Plan. This will be provided by the Government 45 days of contract start.

7.0 MATERIAL. The Government will provide necessary materials to complete this Task Order. The government shall provide necessary office space, for a maximum of 12 contractor personnel at Fort Bragg, NC, a maximum of 2 contractor personnel at Fort Campbell, KY, and a maximum of 1 contractor personnel at Lexington, KY in support of this task, and facilities for storage.

8.0 WORK LOCATIONS. The majority of work will be performed at the following Government sites: Fort Bragg, NC/Fort Campbell, KY/ Lexington, KY. Occasional local travel to affiliate locations for on-site support may be necessary.

9.0 TRAVEL. Travel is required to various continental United States (CONUS) locations to gather data for the performance of the above tasks. The contractor shall travel as initiated by written tasking. It is the responsibility of the contractor to ensure that travel expenses are incurred per the Joint Travel Regulations (JTR).

10.0 HOURS OF WORK. Normal working hours will be required for this effort are 8 hours per day Monday through Friday, within core Command hours which are 0600-1800 Monday through Friday; i.e. The contractor is required to work 8 hours during the 12 hour period of time. There may be periods during which Contractor will be required to work weekends, extended hours, and be on call for mission support.

11.0 PERSONNEL. The Task Order Lead and the Location Leads at 160th SOAR and AROSSA as identified in the Staffing Matrix are considered "key positions". As such, contractor shall submit resumes for all new and replacement candidates proposed.