Performance Work Statement
LIS Theater Operations (TOPS) Post Production Sustainment Support

Contract: W519TC-23-X-XXXX (TBD)

September 2022

Prepared by
Logistics Information Systems (LIS) 441 1st Street
Fort Lee., VA 23831

Table of Contents

1. PURPOSE

The Performance Work Statement (PWS) establishes the requirements for Contractor provided services to include, operations, maintenance, technology refresh, and sustainment support of the (LIS) Theater Operations (TOPS) module to be integrated into the Transportation Coordinators' –Automated Information for Movement System II System (TC-AIMS II). Support of TOPS includes break-fix support, application's test, documentation, and operating configuration management of the enterprise server.

The Contractor shall furnish expert labor necessary to support the Government's requirements for operating and maintaining the TOPS system, interfaces, and providing support to the end-users.

Objectives:

- The Contractor is to ensure the software maintenance and sustainment tasks listed are properly managed in accordance with (IAW) best industry practices and Government regulations.
- The Contractor shall cultivate a business environment that encourages a stable and secure software production baseline for TOPS.
  The Contractor shall ensure system and project documentation is kept current and in a state that permits hand-off to the Government or Government designated Agency / Contractor.

2. BACKGROUND

The current TC-AIMS II Enterprise is used by transportation agents and deploying units to automate the processes of planning, organizing, coordinating, and controlling deployment, redeployment, and sustainment activities worldwide, in times of peace as well as during contingency operations. TOPS provides a modernized, integrated, and easily deployable Automated Information System that supports reengineered functional processes throughout the Department of Defense (DoD). TC-AIMS II links all DoD component unit movement and Installation Transportation Office/Traffic Management Office functionality into a consolidated, integrated, and easily deployable transportation management system.

LIS has a diverse mission that requires an automated capability to provide accurate and timely requirements and real-time visibility of movements to support deployment, redeployment, and sustainment of U.S. forces from within and outside the continental United States (OCONUS) installations and overseas theaters of operations.
TOPS functionality enables movement control elements to manage and coordinate transportation services during Joint Reception, Staging, Onward Movement, and Integration and sustainment operations.

3. SCOPE

The scope of this effort is to sustain the TOPS application software. The Contractor shall provide Post Production Software Support (PPSS) software maintenance for the TOPS application. PPSS software maintenance includes providing fixes, updating software due to regulatory changes, technical upgrades, patches, and providing Software Integration Testing. Maintenance shall be coordinated with the LIS TC-AIMS II Program Management Office (PMO) and shall include updates to the appropriate documentation.

These tasks will include PPSS necessary to support and sustain the TOPS application software, but not limited to:

- General Requirements
- Management Requirements
- Technical Requirements
- Customer Support
- Quality Assurance
- Configuration Management
- Verification and Validation Monitoring
- Deliverables
- Information Assurance / Security
- Performance Metrics

Requirements shall also include overarching activities related to project management, quality assurance, technical analysis, system documentation, and Information Technology (IT) Security.

4. PLACE OF PERFORMANCE

The LIS program office is currently located in Fort Lee, VA. Meetings between the Contractor's support team, principal staff, and LIS personnel shall be held virtually via Microsoft TEAMS or at this location. Work shall be performed at the Contractor's facility and designated locations as identified by the LIS Product Lead (PL) and approved by the Contracting Officer.

5. PERIOD OF PERFORMANCE

Requirement	Period of Performance
Base Period	Date of Award through 12 months
Option Period 1	12 Months
Option Period 2	12 Months
Option Period 3	12 Months
Option Period 4	12 Months
FAR 52.217-8 Extension	6 Months (if required)

6. GENERAL REQUIREMENTS

The Contractor shall provide expert labor necessary to maintain the current baseline of the system and provide software changes and problem fixes to these baselines as required. The Contractor shall comply and keep current with the appropriate DoD, Services, and Army architectures, programs, policies, standards and guidelines (e.g., Risk Management Framework for Security, Net-Centric Enterprise Services (NCES), Department of Defense Information Network (DoDIN).

Requirements shall also include sustainment and documentation for the management, planning, implementation, and regulatory compliance of TOPS. Support services provided under this contract shall include, but are not limited to:

- Software Sustainment and Maintenance
- System Engineering
- Risk Management
- Support to the TC AIMS II integrator (to include the TOPS installer)
- IT Service Management and Cyber Security
- Configuration Management
- Quality Assurance and Testing
- Help Desk
- Database Administration
- Resource Management
- Project Planning and Project Management
- Capacity and Availability Management
- Measurement and Analysis

The Contractor shall maintain the current baseline of the system and provide software change and problem fixes to these baselines as required. The Contractor shall provide to the Government all developed, modified, or converted source modules, processes, programs, scripts, operating instructions, databases, system files, documentation, test files and test conditions used to maintain and sustain each approved systems change request.

The Contractor shall be responsible for its overall responsiveness, cost control, adherence to schedules, technical quality of work, management of Contractor team's efforts and commitment, support equipment and productivity tools and equipment, and to achieving customer satisfaction among TC-AIMS II/TOPS stakeholders.

The Contractor shall provide the methodologies, processes, and capabilities that it proposes to use over the life of the contract. IAW **CDRL A005, Quality Assurance Plan**, the Contractor is encouraged to clearly explain its processes and tools, methods to assure quality, ability to leverage its existing organization and infrastructure (not customize for LIS), and to identify any parameters, limitations, or constraints associated with delivering this functionality.

The Contractor shall optimize the various development, operations, and maintenance activities for the TOPS system. For purposes of this PWS, the term “development” is defined as configuration and coding activities related to the maintenance of TOPS software including bug fixes, and maintenance activity change requests that are not bug fixes, e.g., applying Information Assurance Vulnerability Alert(s) (IAVAs) tests, patches and minor technical mandates (software updates needed to maintain the TOPS module within the TC-AIMS II system as directed by the Government). The covered software activities include not only problem reports, but certain change requests that are maintenance activities. The development and covered activities include, in addition to bug fixes, maintenance activity change requests, e.g., IAVAs, patches and minor technical mandates that TOPS source code is subject to a commercial source code vulnerability scanning tool, and results shall be provided to the Contractor to enhance source code integrity.

6.1 Maintain and Sustain TOPS

The Contractor shall maintain and sustain the TOPS application through the correction of software and system defects identified in test readiness reviews, change requests, problem reports, trouble tickets, and integrating the functionality into the existing TC-AIMS II system.

6.1.1 The Contractor shall meet the Department Information Network (DoDIN) Internet Protocol version 6 (IPv6), Public Key Infrastructure (PKI), Common Operating Environment and all applicable current and emerging DoD and Army regulations. The Contractor shall identify software maintenance activities that arise due to emerging DoD and Army mandates.

6.1.2 The Contractor shall meet DoD information assurance requirements for systems that process “secret,” “Controlled Unclassified Information”, and Privacy Act information.

6.1.3 The Contractor shall meet the DoD requirement for Common Access Card (CAC) enabled user login for the TOPS products. The Contractor shall identify new software maintenance activities that may be necessary to meet DoD requirement for CAC enabled user login.

6.1.4 The Contractor shall maintain all software interfaces, to include interfaces previously developed by the Contractor and interfaces between TOPS and other TC-AIMS II components/modules, as well as maintenance needed to remain compatible with updates to embedded commercial software.

6.1.5 The Contractor shall provide all cyber security support for the TOPS environment; network certification and accreditation activities shall be

coordinated with other Government agencies by a LIS cyber security professional.

6.1.6 The Contractor shall maintain, test, and package systems and software changes to support enterprise configurations

6.1.7 The Contractor shall provide IT support as required to assist with the operational management of the TOPS integration environment.

6.1.8 The Contractor shall utilize the Government provided Army Gold Master for the Contractor hosted test system so that a TOPS production environment is available for support activities.

6.1.9 The Contractor shall identify new software maintenance activities that arise due to emerging DoD and privacy requirements.

6.2 Customer Support

LIS is responsible for providing support to users of TOPS application. TOPS users experiencing problems shall first contact the LIS Service Desk (ASD) Tier 1 Help Desk, (available 24x7x365). The LIS Help Desk shall assess the issue and determine escalation.

The Contractor shall provide a single point of contact that is available to provide technical support for Tier 4 and 5 inquiries during core hours Monday – Friday 0600-1800 EST excluding Federal Holidays. The LIS Subject Matter Expert (SME) shall contact the TOPS SME and provide a ‘hand-off’ of issues/problems to the Contractor’s support personnel.

6.3 Software Modifications

The Contractor shall submit software corrections to the LIS Government-designated configuration management system based on Configuration Control Board (CCB) designated build or patch schedules.

6.4 Maintain Documentation

The Contractor shall submit documentation to accompany all software corrections and code submission. Documentation shall identify the software product, build, and version, and the referenced Problem Report(s) (PR) or Change Request(s) (CR) in addition to the MicroFocus and CAST Inc., scan documentation on all submitted software. The submission shall also include all Documents, TOPS Software User Manual, and TOPS Software Installation Procedures (SIP) updates. (IAW **CDRL A006, Configuration Management**)

6.5 Baseline Integrity

The Contractor shall maintain the current TOPS system baseline and provide software change and problem fixes to these baselines as required.

The Contractor shall ensure that any software fix under this PWS does not compromise the security posture of the TC-AIMS II system.

6.6 Integration Activities

The Contractor shall provide operations and maintenance support of the TOPS software to support integration with the Enterprise Unit Move application.

6.7 Apptricity License Maintenance

The Contractor shall provide Apptricity License Maintenance support to TC-AIMS II per the Settlement Agreement executed on October 24, 2013.

Apptricity Standalone Client Device License for TC-AIMS II means a license to the Apptricity System identified by product code for an unlimited number of user accounts per device and which is utilizable for, but not limited to routine use, production, training, testing, engineering, and/or development software. At present, the TC AIMS II program uses the enterprise server license and stand-alone licenses are not required. See (Appendix 3) for software licenses.

TOPS enterprise server license for TC-AIMS II means a license to the Apptricity System identified by product code for up to 25,000 connected network client users per license and which is utilizable for, but not limited to routine use, production, training, testing, engineering, and/or development software.

7. MANAGEMENT REQUIREMENTS

The Contractor shall be responsible for management of the contract and any associated tasks, projects, and performance. The LIS requirements management process involves protecting, controlling, and maintaining the approved baseline requirements. The Contractor shall track and report changes to the baseline throughout the analysis, maintenance, test, and sustainment phases.

Below is a list of some of the common management tasks expected to be performed on this contract:

- Initial response to LIS on program issues and problems associated with the execution of the contract during core hours (Monday – Friday 0600-1800 EST excluding Federal Holidays.) within 60 minutes after receipt of

a verbal or written request;

- Support by means of Electronic Commerce/Electronic Document Interchange, web access for Contractor-provided information and data;
- Maintain accurate records;
- Provide information to various services and agencies upon approval from LIS;
- Develop and execute a management plan that incorporates configuration and risk management, and provide an approved **Program Management Plan IAW CDRL A001;**
- Report Contractor Manpower Information IAW the paragraph entitled "Contractor Manpower Reporting" (Paragraph 21); and
- Develop and maintain a program management process documented in a formal program management plan.

7.1 Meetings

The Contractor shall be required to attend meetings and coordinate with the Government on a regular basis. Use of teleconferencing and video teleconferencing shall be the standard. Any long-distance travel necessary will require prior approval from COR. Meeting Minutes shall be provided three (3) business days after every meeting between the contractor and the Government. Below is a list of some of the common meetings expected in performance of this contract (this list is not all inclusive): The In-Progress Reviews (IPR) slides shall be submitted to Contracting Officer's Representative (COR) three (3) days prior to the reviews. Any other meeting slides shall be provided to the COR one (1) day prior to the meeting. When required, the Contractor shall participate in Technical Exchange Meetings (TEMs) and other working groups established by the Government. The Contractor's participation in TEMs within the Fort Lee area including travel to LIS facilities shall be covered within the Contractor's overhead (historically monthly). Any long-distance travel required shall require prior approval from PL/Deputy PL LIS. Below is a list of some of the common tasks expected to be performed on this contract:

- Support Ad Hoc Teams
- Support Technical Working Group (TWG)
- Schedule project reviews, and the presentation of the Contractor's vision for creating efficiencies and execution of Tech-refresh requirements: and
- Provide status updates, per the PWS cited requirements

7.2 Weekly Status Meetings

The first weekly Status Meeting will occur no later than ten (10) calendar days following the first week-ending following the performance start date or as required by the Government. Currently, weekly status meetings are held on Wednesday. The starting time for monthly status meetings will be determined by the government COR. However, specific dates shall be determined by the COR in collaboration with the Contractor and adjusted for Holidays, weather, Program activities, events, or for other reasons. The meetings will be primarily conducted via teleconference with

limited meetings on-site at Government location.

At a minimum the Contractor shall provide a monthly report/presentation that includes:

- Schedule Updates
- Testing Updates
- Sustainment Status
- Information Assurance / IAVA Priority and schedule
- Scheduled maintenance outage; Outage occurrences/Incident Reports
- Help Desk tickets status
- Risk Management; and
- Items of importance to the Government.

CDRL (A003): Monthly Status Review/Report

7.3 Integrated Progress Review (IPR)

IAW **CDRL A002, Integrated Progress Review**, The Contractor shall conduct Project In-Process Reviews (IPRs) for Government personnel via video teleconferencing and shall provide formal documentation addressing the Contractor's accomplishments, planned activities, challenges/ risks/issues as well as reports on ongoing projects. The first IPR will occur no later than five (5) business days after contract award, and quarterly (every 3 months) thereafter The Contractor shall prepare and coordinate with the COR, an agenda for all IPRs at least five (5) workdays before a scheduled IPR. The Contractor shall provide the briefing charts to the COR electronically three (3) workdays prior to the day of the IPR. The Contractor shall prepare and coordinate minutes of the IPRs with LIS no later than 48 hours after the IPR. Coordination shall be accomplished through electronic mail. Below is a list of the minimum slides required for the IPR:

- Program Overview
- Issues / concerns
- Accomplishments
- Schedules
- Financials
- Organizations Staffing
- Priorities
- Training / Certifications
- System performance
- System Usage Report

7.4 Working Groups / Integrated Product Teams (IPT) / Technical Exchange Meetings (TEM)

The Contractor shall participate with the Government in multiple teams on an as-required basis. IPTs shall be composed of representatives from all functional disciplines, working together to identify and resolve issues. IPTs shall also make sound and timely decisions, build a successful and balanced program, and make maximum use of timely input from the entire team, including customers and suppliers. The Contractor shall participate on TEMs as required to support TOPS sustainment, maintenance, and integration requirements as determined by the Government. Unless agreed to by the Government in advance, all Contractor costs incurred by participation in TEMs shall be the sole responsibility of the Contractor.

8. TECHNICAL REQUIREMENTS

The Contractor shall be responsible, through its performance, to address and support the technical aspects of the Contract and associated tasks, projects, and performance. Technical activities include the coordinated sustainment of the existing applications. This includes typical software sustainment activities such as maintenance, testing, documentation, and implementation of software releases associated with lifecycle activities. Technical activities address the infrastructural network, hardware, and facility support (as applicable) with full coordination to ensure all levels of information security reliability, and availability, are met and are in compliance with Government regulatory requirements.

8.1 Application Software Maintenance and Sustainment

The Contractor shall maintain and sustain the TOPS application (see Appendix 3 and 4). The Contractor shall perform in-depth requirements analysis and decomposition of all requirements by maintaining a liaison with system stakeholders and users. The Contractor shall maintain the existing TOPS modules.

8.1.1 Software Updates

The Contractor shall develop bug fixes associated with problem reports and software changes associated with maintenance change requests as identified by LIS CCB. The Contractor shall utilize the priority and severity rankings as assigned by the LIS CCB to develop schedules.

8.1.2 Database Maintenance

The Contractor, when required, shall support the TC- AIMS II integrator in database

maintenance activities. These activities shall include performance tuning, incremental software updates, backup and recovery, archiving, control of access permissions and privileges, data security, monitoring disk usage and database performance, reviewing database system logs, problem resolutions, Security Technical Implementation Guide configurations, and IAVA compliant patching. The Contractor shall perform the database corrections associated with problem reports and maintenance change requests as identified by the CCB and directed by the Government. The Contractor shall provide database scripts to perform modifications to the database and resolve problem reports and maintenance change requests as well as to maintain and optimize the database for the system. The Contractor shall utilize the priority and severity rankings as assigned by the LIS CCB to develop schedules. Additionally, systems maintenance activities, specifically IAVAs, shall be coordinated with LIS to the TC-AIMS II integration environment. At no time shall database maintenance/backup activities preclude user access to the system.

8.1.3 Software Installation

The Contractor shall maintain the automated install and de-install capabilities for TOPS that can be used when installing on the enterprise. The install/de- install capabilities for TOPS must install/update/de-install the TOPS module from an existing Enterprise TC-AIMS II installation without degradation to the existing TC-AIMS II system other than removal of the TOPS module in the case of de-installation. The Contractor shall provide instructions to perform the install update and de-install processes, and the Contractor must strictly limit the amount of manual editing of configuration text files required.

8.1.2 Software Documentation

The Contractor shall create and maintain all required technical documentation as well as online help files. This includes, but is not limited to, existing or legacy software design, interface design, system design, DoD Risk Management Framework artifacts, system installation instructions, system user manuals, etc. The Contractor shall provide/update monthly, an Integrated Master Schedule (IMS). All documentation shall be updated and validated with each deliverable to ensure accuracy, relevance and format.

9. Government Acceptance Testing

Technical support is required to support the installation, maintenance, problem resolution of software during Government Acceptance Testing (GAT).

9.1 Test and Evaluation

The Contractor shall provide and identify all, modified, or converted source modules, processes, programs, scripts, operating instructions, databases, system files, documentation, test files and test conditions used to develop each approved maintenance change requests or problem reports.

The Contractor shall be responsible for reviewing Government lab tested and approved interoperability test plans and test results for changes to existing products introduced by Government or third parties into the LIS environment. The Contractor shall inform the Government COR of any problems encountered with implementation of changes to existing products.

9.1.1. The Contractor shall assess the capabilities for each software update/release and employ regression testing (automated and manual) as necessary for each subsequent update/release. The Contractor shall ensure that the testing objectives and success criteria of each Test and Evaluation event are completed before progressing to the next event. The Contractor shall identify any deficiencies in the software operation and performance within the detailed status report, IAW **CDRL A003, Monthly Status Report (MSR).**

9.1.2. The Contractor shall develop processes and procedures for test documentation and verification activities during product testing.

9.1.3. The Contractor shall identify the system changes and develop software test scripts, system installation procedures, testing and maintenance of the software prior to build delivery. A test script/test verifies or identifies if the software change, installation procedures actually work or break something in the code.

9.1.4. The Contractor shall coordinate with the LIS GAT Lab Test Director to verify the following objectives:

a. Identification of the activities required to prepare for and to conduct the product test.
b. Identification of the parties required and responsible for the installation of the product (at a minimum the Government shall have a representative present during all installation activities).
c. Identification of the environment(s) in which the product shall be tested.
d. Identification of the equipment required to conduct the product test.

9.1.5. The Contractor shall conduct component and regression testing to maintain and sustain the current functionality of the TOPS module of the TC-AIMS II specified in this PWS. The Contractor shall test and evaluate IAVA, service packs, and patches to servers for compatibility with TC-AIMS II.

10 KEY POSITION

This section contains information concerning key personnel resources to successfully perform the work requirements. Minimum levels of experience, expertise and educational requirements are specified below.

Project Manager – The Contractor shall identify a Project Manager (PM) to serve as the Government's primary point-of-contact and to provide supervision and guidance for all Contractor personnel assigned to the PWS. The PM is ultimately responsible for the quality and efficiency of the TOPS effort to include both technical issues and business processes. The PM shall be an employee of the prime Contractor. The PM shall assign tasking to Contractor personnel, supervise on-going technical efforts, and manage overall performance. The PM shall be:

e. Qualified, experienced, and accountable for overall program performance;
f. Accountable for delivery, key operations, and technical management of the contract;
g. Accountable for contractual and financial matters of the entire contract;
h. Demonstrate an understanding of Federal, DoD, and Army regulations within the scope of this requirement;
i. Conduct cost and risk analyses, as requested; and
j. Supervise the administrative effort required:
    i. Administer employee relocation and security matters;
    ii. Process appropriate security clearances; and
    iii. Provide general administrative support to Contractors.

The PM shall understand LIS operational and technical requirements as described in the PWS.

The key person specified is considered to be essential to work performance. For this Contract, the Key person shall be assigned for the life of the contract barring circumstances outside the control of the Contractor (e.g., death, disability, etc.).

At least 30 days prior to diverting any of the specified individuals to other programs or contracts (or as soon as possible, if an individual must be replaced, for example, as a result of leaving the employ of the Contractor), the Contractor shall notify the Contracting Officer and shall submit comprehensive justification for the diversion or replacement request (including proposed substitutions for key person) to permit evaluation by the Government of the impact on performance under this contract.

The Contractor shall not divert or otherwise replace the key person without the written consent of the Contracting Officer. The Government may modify the contract to add or delete the key person at the request of the Contractor or Government.

11 OTHER DIRECT COSTS

Other Direct Costs (ODCs), when approved by the Government and incurred by the Contractor in performance of tasks, shall be reimbursed by the Government. The Contractor shall obtain prior approval from the COR for micro purchases (less than $10K) and the Contracting Officer approval for all purchases over the micro purchase level. ODCs include storage, travel, materials, supplies and other supported direct costs. Only actual costs for ODCs that are supported with detail sufficient for the

Government to verify that costs are reasonable and in performance of tasks shall be reimbursed.

12. GOVERNMENT FURNISHED EQUIPMENT (GFE) / GOVERNMENT FURNISHED PROPERTY (GFP)

The Government shall furnish the necessary hardware to perform the required integration and component testing of TOPS. See Appendix 2. Contractors shall provide their own systems, tools, and software necessary to perform administrative and office functions.

Other than GFE/GFP, the Contractor shall provide all resources necessary to sustain TOPS O&M, practices, service assurance, and management. The Contractor shall be responsible for providing all resources necessary to provide the full range of activities related to O&M of the TOPS infrastructure.

13. Reserved

14. QUALITY ASSURANCE

The Contractor shall provide the Government with their Quality Assurance Plan (QAP) and maintain an effective quality control program to ensure services are performed IAW the contract. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality assurance plan is the means by which he assures himself that his work complies with the requirements of the contract.

The QAP shall be delivered NLT 60 days after contract award for acceptance by the Government. The KO may notify the Contractor of required modifications to the plan during the period of performance. The Contractor then shall coordinate suggested modifications and obtain acceptance of the plan by the KO. Any modifications to the program during the period of performance shall be provided to the COR and KO for review and acceptance NLT 10 working days prior to effective date of the change. The Contractor shall revise the QAP within 10 working days from receipt of notice that the QAP is found "unacceptable."

CDRL A005: Quality Assurance Plan (QAP)

14.1 Quality Control Gates

The Contractor shall provide quality control gates throughout the entire Software Maintenance Life Cycle (SMLC), starting with the System Design Document, through software maintenance process, which includes processes such as software coding,

source code control, code reviews, change management, configuration management, and release management. Integrates the organizational information security risk management process- (From Department of Army, PEO EIS, or LIS)- into system development life cycle activities.

14.2 Quality Documentation

The Contractor shall provide quality documentation standards specifying form and content for planning, control, and product documentation that provides consistency throughout the product. Ensure design standards by specifying the form and content of the design product IAW the rules and methods for translating the software requirements into the software design and for representing it in the design documentation.

14.3 Reviews and Audits

The Contractor shall support Government reviews and audits of all services and support provided under this contract. The Government reserves the right to authorize an Independent Verification and Validation (IV&V) of the Contractor's procedures, methods, data, equipment, and other services and support provided at any time during the performance of this contract.

14.4 Conduct Quality Audits

The Contractor shall provide product evaluation and process monitoring that assures the software maintenance, and control processes described in the project's plans, and that the project's procedures and standards are followed. The Contractor shall monitor products for conformance to standards and shall monitor processes for conformance to procedures.

14.5 Unit and Code Inspection

The Contractor shall establish checklist and standards for unit and code inspection and conduct document compliance. An inspection or walkthrough is a detailed examination of a product on a step-by-step or line-of-code by line-of-code basis to find errors. For inspections and walkthroughs, the Contractor assures, at a minimum that the process is properly completed, and that needed follow-up is done. The inspection process shall be used to measure compliance to standards.

15. CONFIGURATION MANAGEMENT (CM)

The Contractor shall work with LIS CM to utilize Solutions Business Manager as a configuration management tool. Solutions Business Manager is a commercial application provided under license to the federal Government. The Government shall provide the Contractor with access and ability to make administrative and configuration changes. Contractor activities include coordinating with the requirements team

concerning changes to software features and developing release plans in association with CM and testing activities. The Contractor shall have subject matter expertise in the Solutions Business Manager toolset with the expertise to manage, maintain and update the software.

Using MIL HDBK 61B, ISO 12207.2017, EIA 649 guidance, and best commercial practices, the Contractor shall institute and maintain a Configuration Management Plan (CMP) to ensure engineering and administrative disciplines (which include configuration identification, configuration control, status accounting, and auditing) are implemented for all development activities. The Contractor shall provide a CMP (see **CDRL A006, Configuration Management**) detailing how it shall identify and maintain the configuration of all work products (to mean baselines as well as other supporting work products); systematically control changes and maintains the integrity and traceability of all work products throughout their lifecycle. The Contractor shall ensure configuration is identified, reliable, traceable, and repeatable, and that all relationships among work products, versions of work products, as well as auditing and reporting on the changes that are made are implemented throughout the development process. The Contractor designated personnel assures that software CM activities are performed IAW the CMP, standards, and procedures.

15.1 CM Monitoring

The CM activities monitored and audited by the Contractor include baseline control, configuration identification, configuration control, configuration status accounting, and configuration authentication. The designated CM manger also monitors and audits the software library. The Contractor CM manager shall assure the following:

- Software configuration identification is consistent and accurate with respect to the numbering or naming of computer programs, software modules, software units, and associated software documents.

- Configuration control is maintained such that the software configuration used in critical phases of testing, acceptance, and delivery is compatible with the associated documentation.

- Configuration status accounting is performed accurately including the recording and reporting of data reflecting the software's configuration identification, proposed changes to the configuration identification, and the implementation status of approved changes. The Contractor shall provide traceability of all Change Requests and Problem Reports through the system lifecycle via a requirement traceability tracking tool.

- Software configuration authentication is established by a series of configuration reviews and audits that exhibit the performance required by the software requirements specification and the configuration of the software is accurately reflected in the software design documents.

- Software libraries provide for proper handling of software source code that can be compiled, executable files, documentation, media, and related data in their various forms and versions from the time of their initial approval or acceptance until they have been incorporated into the final media.

- IAW the LIS CMP, approved changes to baseline software are made properly and consistently in all products and no unauthorized changes are made. Software release candidate numbering shall follow the LIS Release Standards IAW CDRL A006 (Configuration Management).

16. DELIVERABLES

Contractor deliverables include, but are not limited to, software updates, software components, software code, and product documentation to include but not limited to (software user manual, software installation procedures, software administrator guide, software center operations manual).

16.1 Monthly Status Reports (MSR)

On a monthly basis, the Contractor shall deliver a MSR that includes a current sprint burn down chart. The burn chart shall show progress for the previous month and the Report shall identify and discuss upcoming meetings, deliveries, activities accomplished, plan for the next month, new issues, and current issues. The Contractor should highlight those items that are new additions over the previous MSR. The report should also include Transportation Movement Request Tracker and Monthly TOPS IAVA Activity charts. The Contractor shall provide the following deliverable: **CDRL A003: Monthly Status Report** Test Cases and Results.

Test Cases and their derivatives (results, remarks, etc.) shall be documented by the Contractor and submitted to LIS TC-AIMS II System Lead. These test cases include a set of conditions or variables that a tester shall use to determine whether software is working correctly or whether it is not.

Test cases shall be reviewed by LIS and shall also be integrated into an appropriate artifact. Test cases shall, at a minimum, include the following:

- Test case description;
- Test steps;
- Expected results (pass/fail criteria);
- Actual results from test; and
- Remarks.

The Contractor shall document all test results based on the written and approved test plan. For any tests that fail, Contractor shall provide documentation describing the failure and the fix in detail. All failed tests shall be fixed before accepted delivery of the

software.

16.2 Release Notes

Release notes are required with each deliverable. The release notes shall provide details about the delivered software and validate that the Contractor has delivered the expected software to properly deploy and test the software.

16.3 Integrated Master Schedule

The Contractor shall develop, maintain, and submit a monthly Integrated Master Schedule (IMS) that reflects the TOPS inputs to the Program Integrated Master Schedule. Subsequent deliveries shall consist of updates to the Contractor's schedule to maintain the accuracy of the schedule and to track the status and progress of project tasks. If the Government determines that the TOPS IMS requires baseline or milestone date adjustments, the Government shall provide the Contractor with notice of these changes if such changes would impact the Contractor's tasks. If such a situation arises and notice is provided, the Contractor shall ensure that its subsequent monthly IMS update under this CDRL reflects the Government baseline or milestone date adjustment. The Contractor shall provide the following deliverable: **CDRL A007: Integrated Master Schedule (IMS)**.

16.4 Delivery

All deliverables such as, but not limited, to software updates, software components, and software code, shall be ready for compilation and building into the final software products and also include the required script(s) and instructions for building the delivery into the final software products. Deliverables shall include the component or end-product in its entirety, the deliverables shall include script(s) and SIP for installation. **(IAW SOFTWARE RELEASE PLAN CDRL A004).**

The Contractor shall ensure that all software and documentation are delivered electronically if possible. If problems arise that prevent electronic delivery (e.g., network outages), or if the size of the software file(s) is too large thereby preventing a successful download, then deliveries should be made via a DVD(s) to the Product Lead, Logistics Information Systems, 441 1st, Fort Lee, VA 23831 per direction of the Test Readiness Review and BTR process.

Additionally, all source code files should be checked in through the configuration management system. This includes all software licensing requirements (e.g., commercial, open source) and copies of license agreements, if any, for all software products.

Official Government receipt shall be based on the documented signed receipt by the COR for all deliverables by DVD/CD, documented entry of all source code files, metadata database files, installation instructions, and configuration information into the

Government's Source Code Repository; successful demonstration by the Contractor that all delivered code is capable of being compiled, built, and run from the delivery; and successful functional acceptance testing by the Government.

16.5 Software and Data Rights

The Government has unlimited rights to all documents and materials produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

16.6 Schedule, Data Items, and Other Deliverables

In addition, the technical documentation (including specifications and user instructions) for each product shall be delivered for draft and final review prior to submission of the product itself. The Government shall have two weeks to review the draft for comments to Contractor and another two weeks to accept or reject the final product.

17. PERFORMANCE CRITERIA

Performance Criteria are listed in Table 2. Performance evaluation is based on measuring the metrics for management responsiveness, completeness and quality problem identification, timeliness, corrective action plans, effective business relations, and customer satisfaction for all tasks outlined. Performance evaluation of all tasks shall be accomplished every twelve months using Contractor Performance Appraisal Review System by COR surveillance and submittal reviews.

17.1 Evaluation Ratings

The absence of any performance objective and threshold from these performance metrics shall not detract from its enforceability nor limit the rights or remedies of the Government under any provision of the contract. Metrics shall be calculated monthly unless otherwise specified in the monitoring method.

17.2 Performance Requirements

The Contractor's services shall be reported monthly when invoiced based on the service level agreements (SLA) shown in Table 3 within this PWS for the achievement of the full-service levels required. The Contractor shall decrement the monthly invoices IAW these SLAs if the service levels required are not achieved during a service month.

The Government shall not consider any earn-back or credit provisions. The effect of each SLA is cumulative, and the amount used for calculation by the Contractor to determine the amount at risk is 17 percent maximum of the monthly invoice amount.

18. CONTRACT ADMINISTRATION AND MANAGEMENT

The following subsections specify requirements for contract, management, and personnel administration.

18.1 Contract Management

The Contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement.

18.2 Contract Administration

The Contractor shall establish processes and assign appropriate resources to effectively administer the requirement.

18.3 Personnel Qualifications

The Contractor shall, at all times, be responsible for the selection, management, and training of Personnel. Personnel shall be:

- Qualified, trained, experienced and suitable for conditions aligned to job activities acceptable to Government;
- Accountable for overall performance within the scope of their area of responsibility;
- Accountable for delivery, operations, and management within the scope of their area of responsibility; and
- Accountable for contractual and financial matters within the scope of their area of responsibility.

18.4 Personnel Security Requirements

When applicable, Contractor personnel performing services under the contract, task order shall be required to undergo a background investigation. Task Orders may require Contractor personnel to have access to Controlled Unclassified Information (CUI) IAW DoDI 5200.48, AR-25, and the Privacy Act of 1974 (Public Law 93- 579). At a minimum, some CONUS and OCONUS Task Orders will require the Contractor personnel accessing this information to have a favorable National Agency Check with Inquiries (NACI) and/or a DoD Secret clearance (Interim Secret clearances are acceptable). Investigative packages may contain the following forms:

a. SF-85, Questionnaire for Non-Sensitive Positions

b. SF-85P, Questionnaire for Public Trust Positions

c. SF-86, Questionnaire for National Security Positions

d. Credit Report Release Form

e. FD-258, Fingerprint Card

18.5 Information Assurance Training and Certification Requirements

The Contractor's personnel shall meet the following requirements IAW Information Assurance Contractor Training and Certification Requirements as described in Defense Federal Acquisition Regulation Supplement (DFARS) 252.239-7001:

The Contractor shall ensure that personnel accessing information systems have the proper and current certification to perform functions IAW DoD 8570.01- M, Information Assurance Workforce Improvement Program and Army Regulation 25-2.

The Contractor shall meet the applicable information assurance certification requirements, including, but not limited to:

- DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and
- Appropriate operating system certification for technical positions as required by DoD 8570.01- M.

Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing their functions.

18.6 Cyber Security Support

The Contractor shall support the Government with maintenance of the TOPS product within TC-AIMS II. Upon the discovery of TOPS security vulnerability during the cyber security activities (Army continuous monitoring, system scans, audits, program reviews) the Contractor shall work with LIS to provide solutions and develop a plan of action and milestones to address the security finding or vulnerability. The timeline for fixing the vulnerability shall be determined by severity or exploitability of vulnerability and shall be approved by the Government.

18.7 Reserved

18.8 Code Development/Software Policy Compliance

- Contractor shall incorporate the regular use of Software Code Review (SCR) tools, designated in Program Executive Office – Enterprise Information Systems (PEO-EIS) Policy Memorandum #12-65 and its accompanying Standard Operating Procedures, into their own Software Development Lifecycle.
- The Contractor shall provide all developed source code to the Government in sufficient time to review the Software Code Quality/Software Code Assurance (SCQ/SCA) IAW PEO EIS Policy. The Contractor shall provide SCQ/SCA review time in their proposed schedule. At the Government's discretion, the Integrator may be offered an instance of PEO EIS Enterprise tools that can be utilized within their development process and shall be utilized within the formal review process by the PEO. Non-remediated Information Assurance findings shall be accounted for and reported IAW DoD, Army and PEO EIS Policies.

19. TRUSTED ASSOCIATE SPONSORSHIP SYSTEM (TASS)

The Contractor shall ensure compliance with the provisions set forth below. For purposes of this clause, the Government will designate a Trusted Agent (TA), and the Contractor is required to designate a Facility Security Officer (FSO), for this contract. The Government reserves the right to amend or supplement these provisions pursuant to the Changes clause in the contract. 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.

a. In-processing Requirements. Contractor personnel are prohibited from performing services under this award absent compliance with the in-processing requirements set forth below.

(1) For every Contractor employee, the FSO shall provide the following information to the Trusted Agent for input into the Defense Enrollment Eligibility Reporting System (DEERS)/Real-Time Automated Personnel Identification System (RAPIDS) System:

(a) Last Name
(b) First Name
(c) Middle Name
(d) Social Security Number
(e) Date of Birth
(f) E-mail Address (may be either the e-mail address of the incoming individual or the FSO).
(g) Address of Domicile or Residence
(h) Any known aliases or other names the Contractor employee may be also known as (AKA)
(i) Identify any Contractor employee which possesses a Common Access Card (CAC) or other US Government Identification Card from any other agency/service

(2) The DEERS/RAPIDS Systems will send a notice to the e-mail address provided IAW the above requirement, in which the incoming individual's user ID and password are provided. In the event the e-mail message is sent to the FSO, the FSO shall notify the incoming individual of the user ID and temporary password.

(3) The incoming individual shall log into the DEERS/RAPIDS System, and submit an application for acceptance into the System, using the ID and password provided. The incoming individual shall have an active Army Knowledge Online (AKO) account in order to submit the application.

(4) The application will be accepted, returned or rejected by the TA. Notice as to whether the application has been accepted, returned or rejected will be provided to the individual's e-mail address provided in sub-paragraph (1) above, normally within 48 hours after submission. If the application is returned or rejected, the individual shall contact the TA and comply with the TA's guidance to attempt to correct and resolve the issues.

(5) Upon approval of the application, the incoming individual shall receive an e-mail sent to the address in sub-paragraph (1) that the CAC application was approved and to proceed to the Verifying Office (VO) with two photo IDs to obtain a Common Access Card (CAC). For CAC issuance, a DD2842 shall be completed and taken by the individual with two forms of picture ID to the 'then-current-location' for obtaining CAC. The e-mail will contain a URL to download the form. Acceptable forms of ID are: Driver's License, Social Security Card, Military ID, Contractor Company ID with picture and expiration date, VISA charge card with picture imprinted, and passport. The current location of the VO for those personnel working at Fort Lee is:

Fort Lee ID Card Issue Facility/DEERS
Soldier Support Center

1401 B Ave Building #3400
Fort Lee, VA, 23801

Call (804) 765-7636 for hours of operation; appointments are required for all patrons at Fort Lee's ID card office.

For those individuals not working at Fort Lee, contact your TA for information regarding the VO.

b. Revalidation Requirements. The TA is required to revalidate all Contractor personnel, in the DEERS/RAPIDS System, every six months. In the event revalidation is denied, the CAC credentials shall be revoked, and the Card will not be useable to login. In the event any Contractor employee is barred from any US Government installation/facility for any reason, the Contractor management shall immediately notify LIS. In the event any unfavorable information (arrests, police actions, security violations) are discovered by the Contractor management on any Contractor employees, the Contractor management shall immediately notify LIS and a determination of suitability for continued employment will be determined.

c. Out-processing Requirements. When a Contractor employee's performance under this contract ceases, the Contractor or FSO shall provide written notice to the TA. The TA will remove the employee from the DEERS/RAPIDS System. The Contractor shall also ensure that the individual's CAC is turned-in to the Government IAW the out-processing procedures.

20. CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The Contractor shall receive technical direction for future actions and ongoing work efforts from the Contracting Officer's Representative (COR). The LIS will nominate the COR and Contracting Officer will appoint the COR.

21. CONTRACTOR MANPOWER REPORTING (CMR)

The contractor shall report ALL Contractor labor hours (including Subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The Contractor is required to completely fill in all required data fields using the System for Award Management (SAM) web site.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year.

22. CONTRACTOR REQUIRED TRAINING

Each task/delivery order on this contract may have different requirements, resulting in different considerations for AT/OPSEC, etc. The AT/OPSEC coversheet may be included at each task/delivery order, except for supply contracts under the simplified acquisition level threshold ($250,000), field ordering officer actions, and GPC purchases. All items listed below are included in the basic requirements of the PWS, however, an individual OPSEC Standing Operating Procedure/Plan may be required for specific task/delivery orders depending on the AT/OPSEC requirements.

AT Level I Training

All Contractor employees, to include subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training within 14 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The Contractor shall submit certificates of completion for each affected Contractor employee and subcontractor employee, to the COR, or to the Contracting Officer if a COR is not assigned, within 14 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: http://jko.jten.mil

Access and general protection/security policy and procedures

Contractor and all associated subcontractor employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. The Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

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.

Contractors that do not require CAC but require access to a DoD facility or installation.

Contractor and all associated subcontractor employees shall comply with adjudication standards

and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by Government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

AT Awareness Training for Contractor Personnel Traveling Overseas

US based Contractor employees and associated subcontractor employees shall receive Government-provided area of responsibility (AOR) specific AT awareness training, as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

iWATCH Training

The Contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity 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. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance, with the results reported to the COR NLT 45 calendar days after contract award.

Army Training Certification Tracking System (ATCTS) registration for Contractor employees who require access to Government information systems.

All Contractor employees with access to a Government information system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services and must successfully complete the DOD Cybersecurity Awareness prior to access to the IS and then annually thereafter.

Requirement for a formal OPSEC program

The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.

OPSEC training

Per AR 530-1 *Operations Security*, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

Information Assurance (IA)/Information Technology (IT) Training

All contractor employees and associated sub-contractor 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 and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of appointment to IA/IT functions.

Information Assurance/Information Technology 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. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

23. Document List

Description	
Table 1. Referenced Publications	PWS Page 30
Table 2. Performance Criteria	PWS Page (s) 33 and 34
Table 3. Service Level Agreement	PWS Page (s) 35 and 36
Appendix 1. CDRLS	PWS Page 37
Appendix 2. Government Furnished Equipment	PWS Page 38
Appendix 3. Licensed Apptricity Product Module	PWS Page 38
Appendix 4. Gov Owned Software Modules/Capabilities	PWS Page 39

Table 1. Referenced Publications

Unclassified Publications	Available From
1. NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems	Available from the National Institute of Standards and Technology [https://csrc.nist.gov/publications/nistpubs/800- 34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf]
3. DoD 5200.2-R, Personnel Security Program	DoDI 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014; Incorporating Change 3 on September 24, 2020 (whs.mil)
4. DoD Directive 8500.2, Information Assurance (IA)	https://www.prim.osd.mil/Documents/DoDI_8500-2_IA_Implementation.pdf
5. Army Regulation AR 25-2, Army Cybesecurity	Army Publishing Directorate

6. DoD Joint Technical Architecture (JTA), version 6, October, 2003	https://apps.dtic.mil/sti/pdfs/ADA443892.pdf
7. DoD Architecture Framework (DoDAF) Version 2.02	DODAF - DOD Architecture Framework Version 2.02 - DOD Deputy Chief Information Officer (defense.gov)

8. DoD Directive 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense	https://www.dtic.mil/whs/directives/corres/pdf/832007p.pdf
9. Department of Defense (DoD) Net-Centric Data Strategy: Visibility – Tagging and Advertising Data Assets with Discovery Metadata, Memorandum by John Stenbit, October 24, 2003	https://DoDcio.defense.gov/Portals/0/Documents/DIEA/Net- Centric-Data-Strategy-2003-05-092.pdf
10. Federal Information Security Management Act (FISMA)	https://csrc.nist.gov/drivers/documents/FISMA-final.pdf
11. FIPS 140-2 Information Assurance	https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
12. DoD 8570-M Information Assurance Workforce Improvement Program	https://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
13. DISN Connection Process Guide; v5.0, November 2014	DISN_CPG.ashx (disa.mil)
14. DoDI 8510.01, Risk Management Framework	https://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
15. US Army CIO/G6 Information Assurance Best Business Practice (IA BBP); INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION v5.0	https://atc.us.army.mil/iastar/docs/Training_BBP.pdf

16. Defense Disposition Manual 4160.21-M, Instructions for Hazardous Property and Other Special Processing Material	https://www.dtic.mil/whs/directives/corres/pdf/416021_vol4.pdf
Level 1 Antiterrorism Awareness Training	**CAC HOLDERS:** Level I Antiterrorism Awareness Training course (JS-US007-14) is now hosted on the Joint Knowledge Online (JKO) Learning Management System (LMS) for CAC holders at https://Jkodirect.jten.mil. Login and Search for the course on the Course Catalog tab via the number or key word, enroll, and Launch. **FOR NON-CAC HOLDERS:** A standalone version of the course for Non-CAC holders (i.e. Family members 14 years old and over, etc.) is also available at the link https://jko.jten.mil/courses/atl1/launch.html. An access link to this course is also located on the JKO login page. The standalone version is intended for Non-CAC users without a JKO account ONLY! For assistance regarding the Level I Antiterrorism Awareness Training, contact the JKO Help Desk, Monday - Friday 0700-2300 EST at COMM: 757-203-5654 / DSN: 668-5654 or email jkohelpdesk@jten.mil. Our goal is to provide assistance within one business day.

Section 508 Accessibility Standards

The following Section 508 Accessibility Standard(s) (i.e., Technical Standards and Functional Performance Criteria) are applicable (i.e., if box is checked) to this acquisition.

Technical Standards

_X_1194.21 – Software Applications and Operating Systems
_X_1194.22 – Web Based Intranet and Internet Information and Applications
___1194.23 – Telecommunications Products
___1194.24 – Video and Multimedia Products
___1194.25 – Self-Contained, Closed Products
___1194.26 – Desktop and Portable Computers

Functional Performance Criteria

Functional Performance Criteria is the minimally acceptable standards to ensure Section 508 compliance. This block should also be checked to ensure that the minimally acceptable EIT is proposed. The Technical Standards above facilitate the assurance that the maximum technical standards.

_X_1194.31 – Functional Performance Criteria

Table 2. Performance Criteria

Desired Outcome	Required Service	Performance Standard	Monitoring Method	Acceptable Quality Level
Customer Support (PWS 7.2)	LIS Internal Customer Support	96% satisfaction rate as determined by customer surveys	Monthly Reporting	Meets or Exceeds the Performance Standard
DELIVERABLES (PWS 16.)	Meeting LIS Performance Deadlines	96% of all performance requirements met within established deadlines with no issues or notification delays attributable to Contractor negligence or lack of Initiative.	Monthly Reporting	Meets or Exceeds the Performance Standard
Quality Documentation (PWS 14.2)	Quality review of all updated and modified documentation deliverables to include, but not limited to Interface Designs, System Designs, and Database Documentation.	100% of documentation reviewed and 97% free of defects prior to delivery based on total word counts	Project Completion	Meets or Meets or Exceeds the Performance Standard

Desired Outcome	Required Service	Performance Standard	Monitoring Method	Acceptable Quality Level
QUALITY ASSURANCE (PWS 14.)	Improved Service Delivery Processes	100% of Priority 1 and 2 defects are resolved prior to final delivery.	Monthly Reporting	Meets the Performance Standard
SCOPE (PWS 3.)	Project Status Reporting	100% weekly reporting of Milestone execution, defect analysis, development, and test completion including risk analysis, schedule, and task and cost performance.	Monthly	Meets the Performance Standard
MANAGEMENT (PWS 1.)	Effective Business Processes	100% of Level 1 defects acknowledged with a written plan to resolve the issue delivered to the Government within 24 hours. 100% of all Level 2 defects acknowledged with a Root Cause Analysis and a written plan to address the issue within 72 hours.	Monthly Reporting	Meets the Performance Standard

Table 3. Service Level Agreement

Service Level Agreement	Measure	Payment Percentage	Method of Surveillance
SLA # 1. Help Desk Trouble Ticket Resolution Priority 1 and Priority 2. Summarizes the ability of TOPS Help Desk personnel to resolve a specified minimum percentage of trouble tickets received on a monthly basis. * Priority 1& 2 the system is down requires immediate assistance.	98% Trouble Ticket Response for resolution, measured by: The number of Priority 1 trouble tickets responded to or resolved within 24 hours of notification from LIS Tier 2 Manager and Priority 2 tickets responded to or resolved in 72 hours divided by the number of trouble tickets generated by the end of the month multiplied by 100	This SLA represents 2.0% of the total invoice value. 98-100% = 100% of monthly invoice Less than 98% = 98% of monthly invoice*	Validate via a report generated from the Remedy (Team Track) customer system of record shall provide data regarding ticket levels, open/close dates/times, and service duration.
SLA # 2. Help Desk Trouble Ticket Resolution Priority 3 and Priority 4. Summarizes the ability of TOPS Help Desk personnel to resolve a specified minimum percentage of trouble tickets received on a monthly basis.	96% Trouble Ticket Response for resolution, measured by: The number of Priority 3 and Priority 4 trouble tickets responded to within 72 hours of or on-call personnel divided by the number of trouble tickets generated by the end of the month multiplied by 100	This SLA represents 1.0% of the total invoice value. 96-100% = 100% of monthly invoice Less than 96% = 99% of monthly invoice*	Validate via a report generated from the Remedy (Team Track) customer system of record shall provide data regarding ticket levels, open/close dates/times, and service duration.

SLA # 3 Application Software Maintenance Software release meets the release schedule. Functionality of software shall meet required systems architecture and processing capabilities.	Satisfies 100 % of both the Government approved release schedule on time and government approved release requirements.	Meets the scheduled release date as agreed between Government and Contractor. Meets the release requirements as defined and agreed between Government and Contractor.	Government Acceptance Testing (GAT) results.

Appendix 1. Contract Data Requirements List (CDRL)

Cdays = Calendar *Bdays = Business* *NLT = No Later Than*

		Post Award		
		Initial	**Final**	**Updates**
CDRL A001	Program Management Plan	NLT A+20 Cdays	NLT Gov review + 10 Bdays	As Required
CDRL A002	Integrated Progress Review	NLT 5Bdays 1st month ending	n/a	Quarterly
CDRL A003	Monthly Status Report	NLT 2Bdays 1st week ending	n/a	Monthly
CDRL A004	Software Release Plan	NLT A+20 Cdays	NLT 10 Bdays after Gov Review	As Required/ Quarterly
CDRL A005	Quality Assurance Plan	NLT A +60 Cdays	n/a	Monthly
CDRL A006	Configuration Management	NLT A+45 Cdays	NLT A+ 10 Bdays	As required
CDRL A007	Integrated Master Schedule	NLT A+45 Cdays	n/a	Monthly

Appendix 2. Government Furnished Equipment

Item Number	Description	Make	Model Number	Quantity	Serial Number
1	Laptop	Dell	D830	1	CN-OUY141-48643-885-2476
2	Laptop	Dell	D830	1	CN-OUY141-48643-88T-0490
3	Laptop	Dell	D830	1	CN-OUY141-48643-882-4743
4	Server	Dell	R320	1	7BW6C42
5	Server	Dell	R320	1	7BX3C42
6	Server	Dell	R320	1	7BW5C42

(GFP is in a pending status)

Appendix 3. Licensed Apptricity Product Module

The following modules are listed in the software license agreement between Apptricity Corporation and the Department of Defense and comprise the "Framework" for the TOPs transportation management capabilities.

Licensed Apptricity Product Module	
Apptricity Portal	Apptricity Asset Management
Apptricity Schedule Management	Apptricity Supplier Connect
Apptricity Inbound Receiving	Apptricity Service Center
Apptricity Transportation Management Ground	

Appendix 4. Government Owned Software Modules/Capabilities

The below Government owned software modules/capabilities are extended capabilities within the Apptricity Licensed Framework. Any integration of the Government owned software modules/capabilities with the Apptricity Licensed Framework is separate and apart from the support and maintenance provisions of the License agreement cited in Appendix 3.

Government Owned Software Modules/Capabilities (Built on Apptricity framework)	
White Asset Management	Terminal
Transportation Cost Mgmt	Shipment Unit
Exercise Management	ITV (RFITV) Interface
Asset Forecast	Archive
Portal Widgets	