Army Enterprise Staff Management System (AESMS)
Enterprise Task Management Software Solution (ETMS2)
Performance Work Statement (PWS)

Version 1.~~1~~0

~~17 August~~November 23, 2020

THIS PAGE INTENTIONALLY LEFT BLANK

DOCUMENT CHANGE HISTORY

Version	Description of Change	Author	Date
1.0	Initial Document	Mathew Conway	04/03/2020

PREPARATION AND APPROVAL

Prepared By:

Mathew Conway, Project Management Specialist — 3 APR 2020

Approved By:

~~17 AUG~~23 NOV 2020

G. W. Burnside II, Product Lead, Army Enterprise Staff Management System

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Tables

1. SCOPE

This Performance Work Statement (PWS) addresses the need for functional and technical support to meet the demands of the diverse and critical Department of Defense's (DoD) services' and agencies' tasking processes. This solution must seamlessly and electronically exchange information with the Office of the Secretary of Defense (OSD) Correspondence and Task Management System (CATMS) and the predecessor solution, the Task Management Tool (TMT);

Throughout this document, the terms Agency and Agencies will be understood to represent the Department of Defense (DoD) organizations.

The Contractor shall provide the required personnel, supplies, transportation, tools, materials, supervision, and other items and non-personal services necessary to deliver an Enterprise Task Management Software Solution (ETMS2) as a Software-as-a-Service (SaaS) offering and perform the planning, installation, configuration, deployment, accreditation support, training, adoption support, and sustainment as defined in this PWS, except for those items specified as Government- furnished property and services.

The Contractor shall comply with the appropriate Agencies-approved architectures, programs, standards, and guidelines, such as Defense Information Infrastructure (DII), Security Technical Implementation Guides (STIG), DII Common Operating Environment, Defense Information Systems Network, and Shared Data Environment.

This requirement shall cover all DoD agencies across the full spectrum of operations. Each Agency will provide their specific requirements through PEO EIS, PD ES, PL AESMS.

2. REQUIREMENTS

Agencies' diverse lanes of effort produce multitudes of complex tasks and directives that originate and flow through the Agencies daily. The ability to assign, track, and manage a multitude of tasks, which have the potential to become new initiatives or congressional directives, increases operational requirements that propel the Agency staff to increase workflow to meet mission requirements.

The SaaS offering must be a Commercial-off-the-Shelf (COTS) staff action management solution, able to be rapidly deployed, which is interoperable with the ~~OSD~~OSD's CATMS solution~~.~~ and existing instances of TMT. The staff action management solution will be used to provide a seamless fully electronic non-~~-~~reputable tasking and tracking capability which will be used in day to day operations by the Agencies' staff to perform staffing actions, process taskers internal and external to ~~the HQDA~~each Agency, and to interface with OSD CATMS and existing instances of TMT.

Agencies require an ETMS2, which allows management of a tracking and correspondence service and provides a managed service where the Contractor administers the application and database. The ETMS2 is necessary to provide the tools to allow for mission-essential work to be completed and communicated timely, securely,

and according to the proper delegation authority across the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet).

3. PERIOD AND PLACE OF PERFORMANCE

3.1 PERIOD OF PERFORMANCE (POP)

The PoP for this contract shall consist of a twelve (12) month base ordering period with four (4) twelve (12) month option periods.

The PoP start for each customers' requirements shall be defined individually. The POP finish will align with the end of each contract year.

3.2 PLACE OF PERFORMANCE

The work to be performed under this contract shall be conducted at various Agencies' facilities located in the Continental United States (CONUS) and Outside Continental United States (OCONUS) as dictated by each individual customers' requirements. Any support to locations in foreign countries will abide under the standards from the Secretary of State and Status of Forces Agreements (SOFA) or the Technical Expert Status Accreditation/Analytical Support Accreditation (TESA/ASSA) annotated in 6.3.4. The number of personnel needed for each location's software implementation and training will be defined in each customers' requirements. After software implementation and training are complete, on-site full-time employee personnel requirements will be defined by the individual receiving organization and laid out in each customers' requirements. Travel to the hosting environment may be required, at the direction of the Contracting Officer's Representative (COR), to support the Contractor's SaaS assessment and accreditation activities.

During implementation, remote work, telework and virtual/teleconference meetings with customers are authorized where feasible, and in accordance with each customer's specific requirements.

After implementation, personnel providing on-site support may operate in a telework status where feasible and subject to the specific customer organization's operating policies.

Should the Health Protection Condition (HPCON) or Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require or direct changes to the place of performance.

3.3 WORKING HOURS

The Contractor will provide support during the customer- designated, hours, not to exceed forty (40) hours per week, to accomplish the tasks outlined in this PWS including availability to PL AESMS during their core working hours as designated by PEO EIS. The Contractor will coordinate with each customer organization's lead point of contact to determine and provide support during the local working hours and at other times when

necessary. In the event of support for technical maintenance or service outages outside of core working hours, personnel will be on call to support such operations to restore ETMS2 services.

3.4 RECOGNIZED HOLIDAYS

Agencies observe the below listed Federal Holidays. Contractor personnel are not required to provide support on the U.S. Government (USG) holidays as follows:

When a holiday occurs on a Saturday, employees are normally granted the previous Friday as the holiday observance. When a holiday occurs on a Sunday, employees are normally granted the following Monday as the holiday.

- New Year's Day – January 1
- Martin Luther King Day – 3rd Monday in January
- President's Day – 3rd Monday in February
- Memorial Day – Last Monday in May
- Independence Day – July 4
- Labor Day – First Monday in September
- Columbus Day – 2nd Monday in October
- Veterans Day – November 11
- Thanksgiving Day – 4th Thursday in November
- Christmas Day – December 25

4. REQUIRED SERVICES AND TASK MANAGEMENT

The Contractor shall provide a fully functioning, expandable task management software system that operates on the Government's NIPRNet and SIPRNet enabling Agencies' staff to communicate, respond to, and research historical tasks with maximum efficiency and accuracy. Moreover, the ETMS2 must operate within an environment that will facilitate workflows of headquarters and subordinate unit staff to help enable a more streamlined and standardized tasking procedure with increased transparency, visibility, and accountability. The Contractor shall work with each customer to refine command standard operational procedures to streamline the tasking processes. The SaaS offering must be scalable and flexible while leveraging the existing enterprise information technology system infrastructure and providing seamless integration to Microsoft (MS) Windows 10, MS SharePoint (MSSP) compatible servers, and MS Office Suite. The SaaS offering must be capable of being accessed via common internet browsers including but not limited to MS Internet Explorer, Mozilla Firefox and Google Chrome. Additionally, the SaaS offering must be capable of being accessed via government approved mobile devices such as cellphones and tablets via a mobile application.

The ETMS2 must provide an intuitive user experience that reduces or eliminates the need for training. End users should be able to familiarize themselves with the ETMS2 using online training tools. Upon request, the Contractor shall provide Staff Action Training Sessions as defined in the individual customer requirements document ensuring new personnel can proficiently and effectively fulfill assigned task management duties.

Training options can be conducted on-site using group sessions, one-on-one over the shoulder/deskside, Train the Trainer and/or computer-based.

Note: Training requirements will not exceed current operational tempo and expectations of the current task management solution.

The Contractor shall maintain the ETMS2 and related software components and database(s) and provide application administration and Tier 3 help desk support. The Contractor shall work with the Government hosting facility to coordinate any required system administration tasks in the operating environment.

The Contractor shall, at the Government's discretion, migrate or migrate and upgrade existing instances (NIPR & SIPR) of task management related data from the current hosting environment to a Government-owned or Government-contracted hosting environment with minimal disruption of service to users. The migration of data will not include the physical transport of data. The physical transport of data will be managed by Government personnel.

The services and functions to which the Contractor shall fulfill are further defined below:

4.1 FUNCTIONAL AND TECHNICAL SERVICE REQUIREMENTS

The Contractor shall evaluate finalized requirements from Agencies regarding transition planning, and implementation for the ETMS2.

The Contractor shall perform services to support the deployment and/or installation and configuration of a standard task management SaaS offering with the following initial capabilities:

4.1.1 SYSTEM FEATURES

The Contractor shall provide SaaS that allows for effective and efficient tracking management to include monitoring and controlling correspondence, staff taskers, and records through the employment of various functions resident in the system. At Initial Operating Capability (IOC), the ETMS2 shall seamlessly interface with ~~Office of the Secretary of Defense (OSD) Correspondence and Task Management System (~~OSD's CATMS~~)~~, existing instances of TMT, and other instances of the ETMS2. The SaaS offering must provide the ability to communicate, exchange and transmit data and documents, etc. via interorganizational connections between instances of CATMS, TMT and ETMS2 higher departments or commands, to their subordinate departments and commands, and to lateral organizations without loss of data or originating tracking information/identification number. Individual customers will stipulate which interorganizational connections will be required for their instance of ETMS2. The SaaS offering must include a lower to higher echelon correspondence approval process to allow paperless processing of awards, requests, information papers, etc. These requirements are not all-inclusive; specific technical requirements for information technology systems engineering or development are not addressed.

4.1.2 DATA ENTRY

The Contractor shall provide an ETMS2 with the capability to add, update, delete, and view records that are put into the database through a web-based portal or user site. This includes:

- The ETMS2 to control (and related action information), task assignment, status, file, notification, and completion of information for correspondence and action items.
- The SaaS offering shall ensure the updating of data elements is controlled through user profiles (action officer or super user) access levels assigned by the organizational administrator.
- This SaaS offering shall provide the capability for the system to control the update of data elements to specified users within the area of task origination and protect the data from unauthorized updates by subsequent users receiving the tasked item.
- The SaaS offering shall provide super users the capability to delete records from the active system file structure and automatically create an archive record in the database and retain the record in accordance with applicable records management regulations and policies.
- The SaaS offering shall provide the application administrator the ability to retrieve or restore a deleted record from the archived database should the need arise.
- The SaaS offering shall provide user access to data files that are controlled through individual or organizational (group) profiles.
- The SaaS offering shall provide the capability to modify records and data elements specifically identified in the individual user profile.
- The SaaS offering shall provide a version control capability which tracks document changes to the user and group levels to meet auditing requirements and to identify areas which are not performing adequately.
- The SaaS offering shall allow for the creation of individual and group profiles to minimize administrative load to support and sustain user accounts.
- The SaaS offering shall allow for the electronic / digital signing of documents within the environment

4.1.3 TASKING

The Contractor shall provide a SaaS offering for task correspondence and action items to the various levels throughout the chain of command, in a hierarchical fashion from the top of the Agencies to the bottom. The system shall:

- Provide the minimum number of screens or keystrokes required to enter task information and control document routing.
- Provide the minimum number of screens or keystrokes required for General Officers, Department Heads, and Senior Executive Staff members to conduct final review and approvals and/or apply digital signatures.
- Provide users the capability to assign a control item to one or more tasker's agencies/offices to generate a response.

- Provide the capability to assign individuals, groups, and organizations taskers regarding correspondences through defined workflows.
- Provide users the capability to generate a Task Control Document for each tasked item either in a batch mode or automatically by the system upon assignment of the tasked item.
- Provide the capability to generate and queued batch printing of Task Control Documents to be printed one at a time, all at once, or not at all at the user's discretion.
- Provide a single standard format to be used for all Task Control Documents generated by all Agencies within the proposed system, the specific parts of the tasker format shall reflect:
    - The identification of the Agencies office initiating the tasker
    - The type of correspondence being tasked
    - The priority of the response
    - A banner or header appropriately reflecting the type of action
- Provide the capability for specific directions and tasking information to be displayed on the tasker and that this information will change appropriately in accordance with the type of action being tasked.
- Provide the capability to operate in a MS Windows based operating environment.
- Provide the capability to test that the online printer for use is set up the appropriate font set, is online, and ready for input, etc., so that the printer setups are handled in a manner that is transparent to the user.
- Provide the capability that the system will allow for printer setup files for default and optional printers.
- Provide the capability to produce a list of actions that have been tasked to a user and delineates those which have not been acknowledged by recipients and are displayed through the user's inbox and outbox.
- Provide a framework for responding to task and process management challenges, such as personnel evaluations, congressional inquiries, logistics processes, requests for information, and management of Agencies awards and decorations process.
- Provide an easy to use form-based interface that allows all relevant tasker information and responses to be captured.
- Provide (install and configure) an awards and decorations module for use on NIPRNet, which will allow tasking workflows to exist with unlimited users operating within one single task.
- Provide the capability to create subtasks with separate suspense dates within the context of the original task.
- Provide collaboration capability within the task management environment leveraging the MS Office Suite, including MS Outlook.
- Provide suspense dates of accepted tasks, which automatically populate to the users' Outlook calendars.
- Provide managerial interfaces (dashboards) which is separate from that of action officers. This dashboard shall provide task searches, tracking and organization which, will provide management the ability to see current and completed tasks, in

order to monitor work of action officers and collaborate directly with them if required.

- Provide a managerial interface capability to provide metrics on task completion, workload, and work distribution.
- Provide users the capability to leverage privacy and security settings to tasks containing sensitive information.
- Provide the capability to seamlessly leverage the Global Address List (GAL) to assign tasks and conduct user and organizational searches.
- Provide the capability to customize the users' interface with dropdown menus, entry fields, and selection tabs in order to ensure an intuitive user experience for action officers and managerial users. Task lists, collaborative discussion, and metrics must be exportable to MS Excel, MS Word, and MS PowerPoint.
- Provide the capability which has an "out of the box" approval tool, which allows managers to review products from action officers, make corrections, and formally approve, disapprove, concur, non-concur, or make recommendations prior to continuation of workflow.
- Provide users the capability to manage documentation pertinent to their work activities.
- Provide users the capability to attach preexisting documents, scan documents, and import templates to their work items to include MS Office and Adobe documents.
- Ensures the SaaS provided has the capability to auto-generate notifications to the tasking organization, Staff Action Control Office/Officer (SACO), or Congressional Action Control Officer (CACO) for document changes (e.g., extension of suspense date, change in priority or status, or other modifications to a tasking or document package).
- Provide a delegation tree which shows all personnel working on the staff action, to include assignment, timeline, and status of the tasker.
- Provide the capability to customize tasker assignment and routings; no one size fits all solution.
- Provide the capability to have transparency and metrics of workflow bottlenecks, workload comparison, and efficient accountability for staff processes.
- Provide the capability to manage and track multiple correspondence types through standard operational procedures.
- Provide users the capability to take action on correspondence through a tailored user friendly interface.
- Provide users the capability to review/update/edit content on assigned correspondence.

4.1.4 SEARCHES

The solution provided by the Contractor shall provide a SaaS offering which has a search capability and is capable of executing search inquiries by task, user, keyword, subject, and other fields relevant to any given task instance. The solution provided shall also provide the capability to:

- Perform several kinds of searches on data.

- Allow the user to search from many elements within the Master Control Screen.
- Perform searches on selected search criteria by entering partial or full search values as well as ranges of values where applicable.
- Use wildcard characters to enhance search capabilities.
- Display search results in the order of relevance to the search parameters and in the format of a listing containing a single line data for each item located in the search from which the user can select the item to be reviewed in full screen display.
- Include the base tasking document and any associated attachments.
- Restrict other users from viewing sensitive data (Personally Identifiable Information (PII), Personal Health Information (PHI) that may be tracked in the system.
- Have an inquiry restriction listed in the “Viewable by” screen which will restrict access to users not listed on the screen.
- Set and remove inquiry restriction by the user who originally set the restriction.
- Support user selectable-search columns on the Master Control and Search screens for data of the users’ profile and that access has been granted.
- Provide access to correspondences based on the assigned individual, group and/or organization as well as their designated roll in the system.
- Automatically log each action completed in a comprehensive audit history for each correspondence.

4.1.5 NOTIFICATION

The system provided by the Contractor shall allow the users the capability to issue and receive notifications, and shall provide as a minimum:

- The capability for users to issue an electronic notification to other users who have been tasked with action items or are the intended recipients to receive informational copies of correspondence or control items.
- Through the notification capability, users will be notified of status and completion dates for taskers they initiated, are intended for the action officer, or tracking purposes.
- The capability for the system to issue an electronic notification to be made to a designated agency point of contact or to a designated point of entry into an agency. The recipient or point of entry for an agency may be an individual, role, or a valid group ID used by select members of the organization.
- The capability for all users of the Enterprise Email system to be eligible to receive electronic notification of taskers.
- The capability for the system to provide automatic electronic notifications of tasked items to recipients through the use of Enterprise Email.
- The capability that after notification has been received, recipients may review a list of tasks assigned to them as well as the actual Control Document and related information about the action and any documents associated with the action.
- The capability for items assigned at the Action Officer (AO) level, the system automatically generates an assignment status indicating that the AO has received

the action, and the status is displayed on the status screen employed by the tasking officials wishing to verify notification.

- The capability that after reviewing tasked items, recipients may send comments back to the tasking official to the effect that the task has either been tasked appropriately and is being worked or should be reconsidered for tasking elsewhere.
- The capability to provide notifications of taskers when they are received, reviewed, and responded via a user's MS Outlook.
- The capability to provide notifications of new tasks to users, which must transmit to user inboxes via MS Outlook.
- The capability to provide notification to the task originator when the action officer completes a task milestone.
- Transmit and record email notifications that new taskers have been assigned to a tasked individual, group, and/or organization

4.1.6 REPORTING

The system provided by the Contractor shall allow for the capability to conduct standard, customized, or ad hoc query searches and reports which are exportable to all MS applications and Adobe's Portable Document Format (PDF). The system shall produce a variety of reports and query printouts, which assist in the efficient management and control of correspondence, documents, and taskers. The reports shall provide the following:

- The capability that all reports be printable on standard 8 ½ x 11 inch paper.
- The reports to be generated and written to:
    - A print queue for hard copy printing;
    - A file for storage;
    - A display device for immediate viewing, i.e., the user's screen of the personal computer and
    - Emailing to users within Enterprise Email GAL.
- Reporting capabilities that have dashboards that provide key insight into the Agencies' tasker health that highlights overdue and critical taskers that need attention.
- Reporting capabilities that allow ad hoc reporting that is provided out-of-the-box, and can be generated into Excel documents, or presented in custom views, highlighting the status of a tasker, organizations involved, and key decision points.
- Provide comprehensive reporting capabilities to support mission needs. Provide General reports for the Executive Communications and Control, Office of the Joint Defense Affairs, Staff Action Control Officer, and Congressional Action Control Officer. These reports shall meet the parameters outlined in Appendix A
- Special Reports for Office of the Chief Legislative Liaison and Army Audit Agency. These reports shall meet the parameters outlined in Appendix B.
- Suspense reports for super users, which allows creation of multiple suspense reports. The suspense reports shall provide basic information about taskers that are open or overdue.

- Suspense reports should have the capability to be produced for the whole organization, for individual action officers, or a given tasking official.
- Suspense reports shall have the capability to be sorted by control number, suspense date, or action officer. For each suspense report, the user may choose to produce the report using one of the criteria outline in Appendix C.
- The capability to create statistical workload reporting, which allows users to create reports that assist in analyzing assigned workloads. Drawing on collected data allows the capability to create Task Control Document(s), suspense reports sorted in several ways, and monthly workload statistics reports for each organization. Workload statistical reports shall allow the users to produce the reports using the criteria contained in Appendix D.
- Provide administrative and management reports which report all data stored in the database administered and managed by the Contractor to include user lists, unique items, keyword, and open daily.
- Provide custom reports based on ad hoc queries or a combination of standard data elements configured for special reporting requirements. Custom reports shall be limited to super Users, organization administrators, and system administrators.

4.1.7 HELP FUNCTIONS

The system provided by the Contractor shall allow for an online help tutorial about the functions and features comprising the proposed system. The online help shall provide quick, accurate, and easy to understand information concerning how to use the system from the user's perspective. The online help shall provide information to the user that is unfamiliar with procedures such as how to work an action item using the ETMS2.

4.1.8 SOFTWARE CONFIGURATION

The Contractor shall provide the expertise to ~~ensure the solution can~~ execute complex configuration requirements necessary to overlay task management software over manual processes within each Agency and its subordinate organizations.

4.1.9 HOSTING

The Contractor proposed SaaS solution shall include methodology for centralized hosting of their ETMS2 and may include Government or Contractor provided hosting options. Hosting solutions shall be in conformance with the following~~.~~:

Under either scenario, the Contractor will be responsible for managing the application and database instance, to include Information Assurance Vulnerability Alert (IAVA) patch management, addressing STIG requirements, maintenance, upgrades, service management, and service improvements at the application levels. The Government hosting or Government contracted hosting facility will manage the network, storage, and computing infrastructure to include the hypervisor and operating system. The environment for the ETMS2 will be hosted on the Government-owned or Government contracted servers (NIPR and SIPR) at the Government's discretion.

4.1.9.1 GOVERNMENT PROVIDED HOSTING

If Government provided hosting is chosen by the Contractor providing the solution their SaaS offering shall be deployed on both NIPR and SIPR networks within a Government hosting facility, a Government cloud environment, or commercial cloud environment at the Government's discretion. Within a Government provided hosting solution, the Contractor will not manage or control the underlying infrastructure including network, servers, operating systems, or storage, but will have control over the deployed applications and possibly configuration settings for the application-hosting environment. At initial deployment of the solution the NIPR and SIPR environments will be hosted within the Acquisition, Logistics and Technology Enterprise Systems and Services (ALTESS) data center.

4.1.9.2 CONTRACTOR PROVIDED HOSTING

If contractor provided hosting is chosen by the Contractor providing the solution, their SaaS offering shall be deployed within a both NIPR and SIPR cloud environments that is certified to Impact Level (IL)5 and IL6 standards. The Contractor will manage all aspects of the cloud environment to ensure minimal disruption including the deployed applications and configuration settings for the application-hosting environment. If contractor provided hosting is proposed as part of the ETMS2 solution the connection must be routed via a Government Cloud Access Point.

4.1.10 DATABASE MANAGEMENT

The Contractor shall provide database management of the delivered solution:

- The Contractor shall manage and ensure the system has data inputs into the system for both classified and unclassified databases.
- The system shall have status, completion, and file reference information maintained.
- Information input into the system and database shall be input by different users whose access is controlled by a User Profile.
- Allows pertinent data that may be transferred from another control system's database.
- Allows the system to pull from the database a variety of reports and query printouts, which assist in the efficient management, and control of correspondence, documents, and actions.
- Where possible tasking and document management formats will be replicated in a classified management system to increase standardization and maximize user accessibility and familiarity.
- Provides a system comprised of one centralized database containing data from all organizations participating in the system.
- Provide and manage a database which houses data pertaining to correspondence control, staff action, and data regarding physical records.

- The specific data elements comprising the database shall meet the Agencies' standard data dictionary and follow Agencies' standards for element naming conventions.
- Provides and manages a database that is structured in such a manner as to reflect the various level of the Agencies' chain of command from the highest level to the organization, division, branch, and the lowest level, the action officer.
- Provides and manages the database to ensure that data integrity is maintained and enforced at each level, as items are tasked up and down the chain of command without causing unnecessary duplication of data.
- Provides and manages the database to ensure that reference integrity is retained when changes are made to data stored in the database. If this problem is not handled properly, users may lose access to vital pieces of information.
- Be the administrator of the database function at the database software, instance, and database level.
- Provides an enterprise-wide accessible document repository for correspondence attachments for archiving and content management purposes.
- Provides data archiving for the four (4) most recent fiscal years in the active database and up to ten (10) years in the inactive database.
- Provides and ensures that retrieval of information from the inactive database shall not take more than four (4) hours during normal duty hours.
- Provides a capability to interface with a Records Management (RM) system to allow for effective record keeping in accordance with National Archives and Record Administration (NARA) requirements and/or any other agency governing an organization's RM requirements.

4.1.11 MOBILE APPLICATION

The Contractor shall provide a mobile application of the ETMS2 that operates on government approved mobile devices.

4.1.11.1 TECHNICAL SPECIFICATIONS

The mobile application must be

- Compatible with the current DISA approved version of iOS and Android
  - iOS 13x approved 9 December 2019
  - Android 9x approved 6 September 2019
- Must be compatible with the two (2) versions of iOS and Android prior to the currently approved version
- Updated regularly to remain current with future approved versions of iOS and Android to ensure currency before future versions are approved by DISA
- Capable of obtaining authorization for mobile device management

4.1.11.2 FUNCTIONAL SPECIFICATIONS

At a minimum, the mobile application must provide the user the ability to

- Conduct reviews of tasks

- Provide responses to tasks
- Provide approval of tasks
- Digitally sign documents within the task
- Approve tasks
- Approve correspondence
- Close tasks

4.2 SYSTEM ADMINISTRATION

The Contractor shall perform and provide system administration via the utilization of system and organization administrators. In the performance of system administration, the Contractor will be responsible for:

- Overseeing general system performance procedures, including application management and error monitoring.
- Maintaining database and related lookup table.
- Interfacing with designated organization administrators to set up and maintain organization and user profile tables.

The persons designated by the Contractor who meet security requirements and that perform the system administrator and organization administrator functions are the only individuals who will be provided the authority to search the database for deleted records. The Agencies' administrator(s) will work closely with the application administrator to define and set up the organization profile. The organization administrator will be required to have the capability to view the organization profile table, but only the system administrator will have the capability to update it. The organization administrator(s) will have limited authority and capability to set up and maintain user profiles within their own organization in the system. Organization administrators will work closely with the application administrator in performing all system-related tasks as needed.

As application administrators, the Contractor will develop system redundancy and backup protocols to ensure disaster recovery capability. System-level backup procedures will be in accordance with other Agencies' data preservation policies and regulations and will be administered by the Government hosting provider. The Contractor will work with the Government hosting or Government contracted hosting facility to ensure systems will be restored to full operational status within 24 hours of any system outage to include system upgrades or scheduled system maintenance outages.

The Contractor shall ensure the application and the environment will be fully operational with no more than 2% downtime. The maintenance and management plans should ensure that scheduled maintenance and/or upgrades/improvements of the solution will occur outside routine working hours. Scheduled maintenance for upgrades and improvements to the system will not be counted towards the downtime metrics.

The Contractor shall provide comprehensive support of the application environment and coordinate operating environment administration activities with the Government hosting facility.

The system must be capable of supporting the latest industry standards in scalability, flexibility, manageability, and security.

4.2.1 SYSTEM CAPABILITY

The Contractor shall ensure the tasking solution is capable of operating on the NIPRNet and SIPRNet domains and within each domain's technical baseline, in accordance with security standards specified in the DoD Risk Management Framework as defined in Army Regulation 25-2, Army Cybersecurity.

4.2.2 SYSTEM SECURITY, ACCESS RESTRICTIONS, AND PROTECTION

- The SaaS offering should be accredited to process unclassified and classified data.
- The Contractor will provide a current version that has an existing Authority to Operate (ATO) or is capable of being granted an ATO.
- The Contractor will provide comprehensive support to the DoD Risk Management Framework (RMF) processes as defined in DoD Instruction 8510.01. DoD RMF describes the process for identifying, implementing, assessing, and managing cybersecurity capabilities and services, expressed as security controls, and authorizing the operation of Information Systems (IS).
- If Government provided hosting is used, the Contractor shall provide comprehensive support to establish and maintain a Continuity of Operations (COOP) plan supporting a COOP site as part of the requirements to meet and maintain DoD RMF standards.
- All software that is used to build and support the solution must be on the Approved Products List and the entire solution must be capable of obtaining an ATO.
- The security and integrity of the information in the ETMS2 from the application program to the files must be protected from unauthorized access.
- System security, access, and data protection will have redundant features to prevent unauthorized use or release to unauthorized personnel.
- All users must register for system access and enter through a secure portal. The portal will have its own built-in security to ensure users have valid credentials prior to entering the system.
- Each user will be assigned a profile which delineates the access allowed to particular data modules and individual data elements.
- Users may be restricted from accessing specific taskers.
- Provide screen level security that is passed through session variables for users within a particular organization. This shall contain information defining the ability of a user to create, modify, accept, delete, or close records.

4.3 HELP DESK SUPPORT

The Army Enterprise Service Desk (AESD) provides Tier 0 Self-Help Knowledge Articles and Tier 1 System Administrator support required for the duration of this contract. AESD Tier 0-1 support is available to Agencies 24 hours a day, 7 days week, 365 days a year.

The Contractor shall provide any necessary licenses, knowledge articles, and any other documents required to support AESD assuming the Tier 0-1 Help Desk responsibilities.

The Contractor shall provide Tier 3 support to all customers during the duration of this contract in the event of a catastrophic system failure. Optional Remote Tier 2 Help Desk support will be ~~requested~~ordered as necessary within each customers' requirements. Optional Onsite Tier 1 and 2 Help Desk support will be ordered as necessary within each customers' requirements.

After implementation ~~and training~~, optional help desk support will be available Monday – Friday between the hours of 8:00 a.m. and 5:00 p.m. Local Standard/Daylight Time (LST/LDT) except Federal holidays or when the Government facility is closed due to national emergencies, administrative closings, or similar Government directed facility closing.

4.4 TRAINING

The Contractor shall support, as defined in the individual Customer Requirements Document, a deployment of a specified number of users by appropriately allocating training resources to accommodate multiple training classes being conducted concurrently. ~~This offering would be instructor-led training in a hands-on (physical or virtual) classroom environment.~~ The Contractor shall offer, at each customer's request, training modules or training sessions for beginners, advanced users, senior leaders, train-the-trainer, and a tutorial for front office staff oriented on supporting the correspondence and award approval processes.

~~The Contractor shall provide all relevant training materials required, and shall execute a multitier task management software training program for specified users. The Contractor shall further provide a training Program of Instruction (POI) and a training Concept of Operations (CONOPS). These training materials can be provided electronically and printed using each organization's resources. In addition, these training tools must reside within the SaaS offering on both NIPRNet and SIPRNet.~~

~~The Contractor shall provide a System Administrator Training Course to designated staff for each organization in accordance with each customers' requirements.~~

The receiving organizations will afford the appropriate training space and equipment for instruction. The Contractor shall complete training in accordance with each customers' requirements.

The Contractor shall provide all relevant training materials required, and shall execute a multitier task management software training program that allows for:

- Self-paced Computer Based Training (CBT),
- Virtual instructor-led training, and
- In-person Instructor-led (traditional classroom style) training

All methods of the training shall provide adequate information and instruction to ensure that end-users are able to intuitively use the ETMS2. At the end of the training, users must, at minimum, be able to:

- Create a task
- Task an action
- Accept an action
- Respond to an action
- Close an action
- Search for an action
- Run reports.

Additionally, senior leaders and their staff must be trained on how to perform the correspondence and award approval process.

~~The Contractor shall provide self-paced Computer Based Training (CBT).~~ The Contractor shall provide a System Administrator Training Course to designated staff for each organization in accordance with each customers' requirements.

The CBT modules will be for action officers, staff action control officers, congressional action control officers, and senior leaders (correspondence and award approval process focused). The CBT training must be for both beginners and advanced users. The CBT should be delivered via a software product installed over the internet as web-based training. Web-based training shall be accessible to those with a Common Access Card (CAC) who have been issued a license for the ETMS2. The web-based training also needs to establish the new user's account once the training is complete. Upon successful completion of the CBT, the ~~system~~training module must generate a certificate of completion.

The Contractor shall further provide a training Program of Instruction (POI) and a training Concept of Operations (CONOPS). These training materials can be provided electronically and printed using each organization's resources. In addition, these training tools must reside within the SaaS offering on both NIPRNet and SIPRNet.

5. SECURITY REQUIREMENTS

5.1 SECURITY CLEARANCE REQUIREMENTS

The Contractor personnel performing work under this contract shall possess an active SECRET or TOP SECRET clearance as applicable by the requiring Agencies at the time of the proposal submission, and shall maintain the level of security required for the life of the contract. At a minimum all personnel will have a SECRET clearance while some Contractor employees will need to have TOP SECRET to enter secure workspaces to provide training and consultation services to some customer organizations. Those personnel requiring above SECRET will be identified in each new customer's requirements at the time the RFP for that customer is released.

All Contractor personnel accessing Government networks must meet the qualifications described in DA Pamphlet 25-IA, Information Assurance (IA). The link for the DoD IA awareness training is https://cs.signal.army.mil.

All Contractor personnel shall be vetted in advance of an appropriate Agency background investigation for the proper security clearance required prior to being granted access to any Agencies' computer system(s), either directly or remotely. The COR shall have the authority to verify all clearance levels and authorities. The nature of this PWS requires access to the agency's unclassified and classified systems.

The Contractor's assigned responsibilities mandate access to classified spaces. All Contractor and Subcontractor personnel who will perform work on-site are required to possess a Secret or Top Secret clearance. Contractor personnel must be US citizens and possess at least an active security clearance to begin work on this effort. Additional security requirements will be stipulated in the DD Form 254 to be provided by the Government ~~at contract award~~.

The Contractor and all associated Subcontractor employees shall comply with applicable installation, facility, and area commander installation and facility access and local security policies and procedures (provided by the USG representative). The Contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished 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 Agencies and/or local policy. Should the Health Protection Condition (HPCON) or Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

The work performed for this contract may be up to the SECRET and/or TOP SECRET level, as determined by the USG. The need for TOP SECRET clearance level shall be outlined within individual customer's requirements.

Violations or spillages of classified information as a result of non-compliance may result in government requesting the personnel responsible for violation or spillage be removed from the program immediately.

5.2 PHYSICAL SECURITY

The Contractor shall be responsible for safeguarding all Government equipment, information, and property provided for Contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured.

5.3 ACCESS CONTROL BADGES

The Government will be required to provide access control badges to Contractor personnel who will be working on this project within designated/controlled areas.

The Government Representative is responsible for issuing access control to the Contractor as part of the organization's In/Out-Processing Procedures. Under no circumstances will Contractor personnel loan/give their access badge/keys to other personnel or to visitors to use to access/enter buildings belonging to the Government. Contractors shall immediately report lost or stolen access control badges to the organization's Security Manager and the AESMS program office.

The Contractor personnel who need to facilitate immediate access to any Agencies building or who have questions about their authorized access will contact their first line supervisor. A visitor is defined as anyone without an Agency authorized access control badge access to the facility/area.

5.4 ACCESS TO FACILITIES

The Government, when required and deemed necessary, will authorize appropriate badge access to Contractor employees identified on the Contractor's personnel roster, wearing identification badges, and complying with Installation and organizational security procedures. The COR will maintain facilities access control approvals.

5.5 KEY CONTROL

The Contractor shall establish and implement methods of ensuring all keys or key cards issued to The Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to The Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys or key cards to the Contracting Officer (KO).

In the event keys, other than master keys, are lost or duplicated, the Government, at its option, may replace the affected lock or locks or perform rekeying. When the replacement of locks or rekeying is performed by the Government, the total cost of rekeying or the replacement of the lock or locks may be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system will be replaced by the Government, and the total cost may be deducted from the monthly payment due the Contractor at the KO's discretion.

The Contractor shall ensure the use of Government issued keys or key cards are not used by any persons other than the Contractor's employees. The Contractor shall ensure that employees do not open locked areas to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the COR.

5.6 ANTITERRORISM (AT), OPERATIONS SECURITY (OPSEC) AND INFORMATION ASSURANCE (IA)

5.6.1 AT LEVEL I TRAINING

All Contractor employees, including Subcontractor employees, requiring access to Government installations, facilities, or controlled access areas, shall complete AT Level I awareness training within thirty (30) calendar days after the contract start date. The Contractor shall submit certificates of completion for each affected Contractor employee and Subcontractor employee to the COR within five (5) calendar days after completion of training by all employees and Subcontractor personnel. AT Level I awareness training is available at https://jko.jten.mil/.

5.6.2 AT AWARENESS TRAINING FOR CONTRACTOR PERSONNEL TRAVELING OVERSEAS (IF APPLICABLE)

The Contractor and its associated Subcontractor must make available to its employees and receive Government-provided AT awareness training specific to the Area of Responsibility (AOR) as directed by AR 525-13. Specific AOR training content is directed by the combatant commander, with the unit AT Officer being the local point of contact.

5.6.3 ACCESS AND GENERAL PROTECTION/SECURITY POLICY AND PROCEDURES

The Contractor and all associated Subcontractor employees shall comply with applicable installation, facility, and area commander installation/facility access and local security policies and procedures (provided by the Government Representative).

The Contractor shall also 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 as directed by Agencies, and/or local policy. In addition to the changes otherwise authorized by the Changes Clause of this contract, should the HPCON or FPCON at any individual facility or installation change, the Government may require changes in Contractor security matters or processes.

5.6.4 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 Government will issue the Contractor employee a CAC only if duties involve one of the following:

- Both physical access to a Government facility and access, via logon, to Agencies' networks on-site or remotely.
- Remote access, via logon, to an Agencies' network using Agencies approved remote access procedures.

- Physical access to multiple Agencies' controlled facilities on behalf of the Agencies on a recurring basis for a period of six (6) months or more. At the discretion of the sponsoring activity, the Government may issue an initial CAC based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

CACs are issued for a 3 year increment, however Contractor employees shall surrender their CAC to the Government

- Immediately prior to departing or being terminated from work related to this contract.
- Within 48 hours of the conclusion, expiration or termination of this contract.

5.6.5 CONTRACTORS THAT DO NOT REQUIRE CAC, BUT REQUIRE ACCESS TO A DOD FACILITY OR INSTALLATION

Contractor's and all associated Subcontractors' 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 the status of forces agreements and other theater regulations.

5.7 IWATCH TRAINING

The Contractor and all associated Subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Antiterrorism Officer). This training is 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 thirty (30) calendar days of contract award, and within five (5) calendar days of new employees' commencing performance, the results shall be reported to the COR No Later Than (NLT) five (5) calendar days after contract award.

5.8 CONTRACTOR EMPLOYEES WHO REQUIRE ACCESS TO GOVERNMENT INFORMATION SYSTEMS

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

5.9 OPSEC STANDING OPERATING PROCEDURE (SOP)/PLAN

The Contractor shall develop an OPSEC SOP/Plan within ninety (90) calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan will include the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the Contractor shall identify an individual who will

be an OPSEC Coordinator. The Contractor will ensure this individual becomes OPSEC Level II certified per AR 530-1.

5.10 OPSEC TRAINING

Per AR 530-1, Operations Security, new Contractor employees must complete Level I OPSEC training within thirty (30) calendar days of their reporting for duty. All Contractor employees must complete annual OPSEC awareness training.

5.11 IA/INFORMATION TECHNOLOGY (IT) 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 and Army training requirements in DoDD 8570.01, DoD 8570.01-M, and AR 25-2 within six (6) months of employment.

5.12 IA/IT 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.

5.13 HANDLING OR ACCESS TO CLASSIFIED INFORMATION

The Contractor shall comply with FAR 52.204-2, Security Requirements. This involves access to information classified "Confidential," "Secret," or "Top Secret" and requires all Contractors and its employees to comply with:

- The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M)
- Any revisions to DoD 5220.22-M, notice of which has been furnished to the Contractor.

5.14 THREAT AWARENESS REPORTING PROGRAM (TARP)

For all Contractor employees with security clearances per AR 381-12 TARP, Contractors must receive annual TARP training by a counterintelligence agent or other trainer. The Contractor shall provide a certified list of all contract personnel and date of completion. Training will be scheduled within thirty (30) days from contract award.

6. ADMINISTRATIVE REQUIREMENTS

6.1 INVOICING

The contractors shall submit two (2) invoices each month for work performed the prior month. Both invoices will be received by the COR by the (fifteenth) 15th calendar day of the month.

The first invoice will cover the details of travel expenses. The invoice for travel expenses will be accompanied by all travel receipts. Travel must be itemized by Individual and Trip. Each trip should reference the Travel Approval Request Number it was approved under, and be accompanied by receipts related to the travel being claimed.

Travel shall be approved per the terms and conditions of each customers' requirements. Signed/approved TAR forms shall be submitted with the invoice, and all receipts for airfare, rental car, lodging, and all receipts directly being charged for expenses over $25.00 shall be submitted as support/back up documentation with the invoice submittal. No payment will be made without documentation/receipts. No payment will be made for travel that is nonconforming to the Federal Travel Regulations (FTR). No payment will be made for travel that was not approved in advance.

The second invoice will be for all other Contract Line Item Numbers (CLIN) billed against in the preceding month. The contractor may invoice only for the hours and unique services ordered by the government and actually used in direct support of the client representative's project.

The invoices shall be submitted on official letterhead and shall include the following information at a minimum:

- Contract Number
- Remittance Address
- Period of Performance for Billing Period
- Point of Contact and Phone Number
- Invoice Amount
- ~~Skill Level Name and Associated Skill Level Number (for Time and Material (T&M) or Labor Hour)~~
- ~~Actual Hours Worked During the Billing Period (for T&M or Labor Hour)~~

NOTE: The Government reserves the right to audit; thus, the contractor shall keep on file all backup support documentation for travel and Other Direct Costs (ODC).

6.2 CONTRACTOR IDENTIFICATION REQUIREMENTS

In accordance with FAR 37.114(c), all Contractor personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious are required to identify themselves as such to avoid being mistaken for Government officials. Contractors performing work at Government workplaces shall provide their employees with an easily readable identification (ID) badge indicating the employee's name, the Contractor's company name, and a recent color photograph of the employee. Contractors shall require their employees to wear the ID badges visibly when performing work at Government workplaces. Contractor personnel shall also ensure that all emails, documents, or reports they produce are suitably marked as Contractor products and/or that Contractor participation is appropriately disclosed. All signature blocks on emails shall indicate that the sender is a Contractor employee and include the Contractor's company name.

6.3 TEMPORARY DUTY TRAVEL

Travel may be required, by direction of the COR, to the hosting data center to support the ETMS2 system's assessment and accreditation activities, and implementation and training, and to other CONUS and OCONUS locations and facilities to support implementation and training. Travel costs will be considered reasonable and allowable to the extent they do not exceed on a daily basis, the maximum per diem rates in effect at the time of travel. The Joint Travel Regulations, while not wholly applicable to Contractors, shall provide the basis for the determination as to reasonable and allowable. Other Direct Cost CLINs ~~Travel~~ shall be ~~a cost reimbursable~~ established for travel expense. Per the SECDEF Efficiency Memo, dated 14 Mar 2011, All DoD travel requests MUST include a justification that alternate means (VTC, SVTC, web-based communications, or teleconference) are not sufficiently able to accomplish travel objectives.

A TDY at one location may not exceed 180 consecutive days except when authorized by the appropriate authority. Issuing a TDY order for 180, or fewer, consecutive days, followed by a brief return to the Permanent Duty Station (PDS) and then another TDY order for return to the same location, is a violation of the 180-consecutive-day policy if the known, or reasonably anticipated, TDY duration exceeded 180 days when the initial order was issued. Bona fide assignment extensions that, when added to the originally authorized TDY period, total more than 180 days at one location, may be directed by the AESMS Program Office only when necessary for unforeseen changes or delays.

- The Contractor shall make its own travel arrangements.
- Daily commuting expenses are not considered reimbursable.
- Local travel costs will not be allowable.
- Costs for transportation may be based on mileage rates, actual costs incurred, or a combination thereof provided the method used results in a reasonable charge.
- Maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours.
- When authorized to drive a personally owned vehicle in lieu of lowest available customary standard coach or equivalent airfare, mileage will be authorized between the regular worksite and the TDY location; however in and around mileage at the TDY location will not be authorized. A Constructive Comparison Worksheet will be required to show cost comparisons between travel modes.
- When authorized mileage in conjunction with temporary duty, the Defense Table of Official Distances will be used to calculate distances between departure and arrival locations.
- Any long-term Temporary Duty (TDY) for a duration of 31-180 days at a single location is authorized at a flat rate of 75% of the locality rate, payable for each full day of TDY at that location.
- Any long-term TDY for a duration of 181 days or more at a single location is authorized at a flat rate of 55% of the locality rate, payable for each full day of TDY at that location.

For authorized travel cost reimbursable, the Contractor shall account for cost in accordance with the FAR, and FTR. All necessary travel meeting the above criteria shall be submitted and approved in accordance with the attached AESMS ETMS2 Contractor Travel Process. Exceptions to these guidelines shall be approved in advance by the KO or their Designee.

6.3.1 TRAVEL APPROVAL REQUESTS

The Contracting Officer's Representative will be the approval authority for all travel. All travel will require a Travel Approval Request (TAR). TARs shall be submitted twenty-one (21) calendar days prior to the start date for requested travel. The Government will approve travel NLT (fourteen) 14 calendar days prior to the start date of the requested travel. TARs requesting a deviation from the lowest available customary standard coach or equivalent airfare accommodations shall include a cost comparison worksheet.

6.3.2 PROCESSING REIMBURSEMENT FOR TRAVEL

Upon completion of travel, travel claims with all necessary receipts to justify expenses shall be submitted within seven (7) calendar days for review and will be accounted for in the travel invoice within two (2) billing periods. All Travel Claims should be submitted to the ETMS2 COR within fifteen (15) calendar days for review prior to invoice submission. This ensures the level of accuracy required for timely invoice reconciliation.

After travel is incurred, documentation/receipts shall be sent to the COR (with the invoice submittals).

NOTE: NO PAYMENT WILL BE MADE WITHOUT DOCUMENTATION/RECEIPTS.

6.3.3 OCONUS TRAVEL

In the event that a customer's requirements require the contractor's presence on-site at an OCONUS location; the Contractor will be responsible for identifying ALL costs associated with mobilizing and living expenses for all OCONUS personnel in the proposals for each customer's implementation/request for service. An Other Direct Cost ~~cost reimbursable~~ CLIN will be established for each OCONUS location. The Contractor may use DoD Standardized Regulations (DSSR) allowances, as a guide in developing its Firm Fixed Price (FFP) proposal. The contractor shall include all costs such as airfare to and from the employee's home station, housing (which includes power, lighting, furniture rentals, internet, phones, and sewage), security, all transportation costs, leases, cost of living adjustments, uplifts, VISAs, work permits, sponsorships, medical/dental examinations, recruitment and retentions incentives, quarter allowances or any other costs and allowances not specifically detailed in the PWS. Mobilization may include travel to CONUS Replacement Center (CRC) from an individual's home of record prior to deployment. Travel for CRC will be conducted in accordance with the travel policies outlined in paragraph 6.3~~.~~

NOTE: The Government may provide for Contractor employees working in Korea a U.S. Forces Korea (USFK) Sponsoring Agency (SA) and Responsible Officer (RO) In Accordance With (IAW) USFK REG 700-19. However, the Government will not incur any

costs for the Logistics Support Privileges defined in the USFK Regulation 700-19. Privileges may be provided if the Contractor employees and authorized dependents are properly authorized, on a space-available and non-reimbursement basis.

6.3.4 SPECIAL COUNTRY REQUIREMENTS FOR OVERSEAS PERFORMANCE

The Contractor must comply with applicable Host Nation laws and regulations in accordance with the terms and conditions of the contract and secure applicable permits prior to contract performance. Contractors traveling OCONUS for TDY shall refer to the Electronic Foreign Clearance Guide for the applicable country at https://www.fcg.pentagon.mil/fcg.cfm for information on entry requirements. The Contractor is responsible for ALL the requirements of doing business for all OCONUS locations. Below are examples of some of the special OCONUS performance requirements:

6.3.4.1 EUROPE SPECIAL REQUIREMENTS

The Contractor shall assign personnel to Europe in accordance with KO guidance. All such assignments shall comply with the following: Army in Europe Regulation 715-9 Contractor personnel in Germany - Technical Expert, Troop Care, and Analytical Support Personnel.

Contractors traveling to Germany for TDY shall use the TESA/ASSA TDY procedures. The complete instructions are available at the DOD Contractor Personnel Office (DOCPER) website at https://www.eur.army.mil/contractor/ Under the Technical TESA/ASSA TDY procedure, Contractors would be entitled to logistical support and applicable tax exemptions.

Before the Contractor begins work in Germany, the COR for the Contractor seeking TESA/ASSA under this procedure will complete the TESA/ASSA TDY Application online, Page 88 of 98 through the DOCPER Contractor Online Processing System (DCOPS) and submit it, along with required uploaded documents to DOCPER. The application form (AE 715-9D) must be printed from DCOPS, signed by the COR and the applicant, and then be scanned and uploaded into DCOPS.

6.3.4.2 KOREA SPECIAL REQUIREMENTS

U.S. Government contractors who travel to the Republic of Korea (ROK) must be identified as Invited Contractors/Technical Representatives (IC/TR). Reference is United States Forces Korea (USFK) Regulation 700-19 (The Invited Contractors and Technical Representatives Program). Under the SOFA, theater clearance is required.

The COR will inform the KO of any anticipated contractor travel to Korea as soon as the requirement is known. The COR will ensure that the SA has been identified to the COR, and that the SA has appointed a RO. The RO shall ensure the completed USFK Form 700-19A-R-E and Letter of Accreditation (LOA) are submitted USFK/FKAQ NLT thirty (30) business days prior to travel. USFK/FAQ will review, process, stamp, and complete Part III of the USFK Form 700-19A-R-E.

SOFA status ensures that SOFA provisions on legal and jurisdictional issues and official support mechanisms are applied to the Contractor while on official business. In order to obtain SOFA status in Korea, the Contractor employees shall present a DoD identification card obtained stateside prior to travel, passport with A-3 Visa, LOA, red-stamped USFK Form 700-19A-R-E, and copies of each document to Korean immigration authorities.

6.3.4.3 JAPAN SPECIAL REQUIREMENTS

The SOFA with Japan covers contractor personnel who travel to Japan solely to execute contracts for the benefit of the United States armed forces. Under the SOFA, theater clearance is required.

6.3.4.4 SOUTHWEST ASIA (SWA) SPECIAL REQUIREMENTS

The North Atlantic Treaty Organization (NATO) SOFA with SWA covers contractor personnel who travel to SWA solely to execute contracts for the benefit of the United States Armed Forces. Under the SOFA, theater clearance is required.

The Contractor shall ensure and provide necessary instructions for personnel accessing and completing training requirements. SWA has many stringent and complex laws that hamper bringing employees into the country. It is the sole responsibility of the Contractor to ensure it has the knowledge and capability to fully deploy personnel into SWA, such as obtaining the necessary business license, this includes full functionality such as driver's licenses, etc. or the sponsorship/teaming company business license required for doing business in a specific country.

6.3.4.5 AREA/THEATER CLEARANCE

Where an area or theater clearance is required, the Contractor shall submit clearance requests via the Aircraft and Personnel Automated Clearance System (APACS). . The Contractor shall log onto the website at https://apacs.milcloud.mil/apacs/ to create an account, and then create and submit a clearance request. Training, materials, documentation, and contact information is available on the website.

6.3.4.6 CONTRACTORS AUTHORIZED TO ACCOMPANY THE FORCE.

Compliance with DFARS Clause 252.225-7040, Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed OCONUS, is required.

6.3.5 DFARS CLAUSE 252.225-7043, ANTITERRORISM/FORCE PROTECTION FOR DEFENSE CONTRACTORS OUTSIDE THE U.S.

This clause applies to both contingencies and non-contingency support. The key antiterrorism requirement is for non-local national Contractor personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the Contractor's compliance with combatant commander and subordinate task force commander policies and directives.

7. PERSONNEL

The Contractor shall at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facilities are not closed for recognized holidays. During times of local, national or global crisis, the Contracting Officer will issue specific guidance related to continuing or suspending support related to the SaaS offering, and all or specific customers affected by the crisis.

7.1 PERSONNEL MANAGEMENT PLAN

The Contractor shall develop a Personnel Management Plan that demonstrates an ability to:

- Provide quality personnel
- Ensure adequate staffing during the duration while minimizing the impact of turnover
- Ensure efficient replacement of all KEY personnel as necessary
- Describe how security clearance requirements are met
- Describe the process to recruit and retain a qualified and capable workforce that can accomplish the entire scope of the effort outlined in the PWS are addressed and that the methodologies and/or approaches are acceptable.

7.2 PERSONNEL SKILL QUALIFICATION AND REQUIREMENTS

The Contractor shall demonstrate a management methodology in order to recruit, sustain, and maintain the expert personnel to meet a successful execution of all requirements of the PWS throughout the period of performance.

The Contractor shall assign sufficient resources and technically qualified, well trained personnel to accomplish the tasks outlined in this PWS. The Contractor shall assign qualified personnel to accomplish these tasks while operating in an effective, efficient, and timely manner. All Contractor personnel assigned to this effort shall be qualified IAW all contract terms and conditions.

No personnel position providing contracted support shall remain vacant for more than fifteen (15) business days, unless in an OCONUS location, then the position shall not remain vacant for more than thirty (30) business days. The Contractor may provide a temporary substitute, provided the substitute meets or exceeds the qualifications of the personnel being replaced. Permanent replacement personnel shall have equal or superior qualifications to the personnel being replaced.

7.3 KEY PERSONNEL

Key personnel are expected to perform the necessary duties aligned with their position and to be available to the Government during the core working hours, however, there is no requirement for key personnel to be collocated with the Government. Key Personnel may be required at times to travel to AESMS Government workspace to conduct business. The following personnel are considered key personnel by the Government:

1. Program Manager – The Contractor shall assign a program manager for this project that will interface with the AESMS Program Office on the overall contract. This includes human resource management, risk identification and management, project scheduling, and customer project reporting. A Program Manager shall be qualified to perform such tasks as:

    - Organizes directs and manages contract operation support functions, involving multiple, complex, and interrelated project tasks; plan and manage the work of information systems project teams.
    - Manages teams of contract support personnel at multiple locations.
    - Maintains and manages the government interface at the senior levels
    - Meets with AESMS personnel to formulate and review task plans and deliverable items.
    - Ensures conformance with program task schedules and costs.
    - Design and implement information and security standards.
    - Manage contract requirements.
    - Required to attend technical interchange meetings.
    - Manages travel requirements for CONUS and OCONUS locations.
    - Formulates and review deliverables.
    - Manages and track budget financials.
    - Provides program management support to Contractor team.

2. System Engineering Lead – The Contractor shall assign a system engineering lead for this program that will act as a primary point of contact with the AESMS Program Office on the overall technical solution such as:

    - Oversees application and system compliance with all DoD security requirements.
    - Coordinates design and scale of all application environments and their dependencies across all networks (NIPR/SIPR).
    - Manages integration with any and all externally hosted environmental dependencies needed for the application to function.
    - Coordinates all system and application maintenance.
    - Manages all platform upgrades for customer-facing application and all dependencies.
    - Supervises all system backup and restoration procedures.
    - Reports all incidents to the COR and facilitates their resolution.
    - Acts as primary technical point of contact for all Tier 3 incidents reported by end-users and their resolution.
    - Manages application installation and initial configuration for each customer
    - Manages migration of existing customer data that moves into the application environment.

No key personnel position shall remain vacant for more than ten (10) business days. The Contractor may propose a temporary substitute by providing a resume of the substitute personnel, provided the substitute meets or exceeds the qualifications of the personnel being replaced. In addition, the Contractor shall supply any additional information

requested by the Contracting Officer. Proposed permanent replacement personnel shall have equal to or superior qualifications to those personnel being replaced. The Contracting Officer will notify the Contractor within five (5) business days after receipt of all required information of the consent on replacement personnel.

7.4 CONTRACTOR PERSONNEL AND WORK AREAS

Contractor personnel working in Government facilities shall have a professional demeanor and dress in appropriate business attire.

The Contractor shall maintain clean and orderly operational areas and observe the following practices:

- Empty boxes and other debris shall be removed from the area.
- Smoking is prohibited in all areas inside of Government facilities, as well as directly in front of Government buildings. This includes any smokeless tobacco and electronic cigarettes. Smoking is only authorized in designated areas.
- Eating or drinking is prohibited in areas posted.
- All Contractor personnel assigned to these tasks must be able to read, write, speak, and understand the English language.

7.5 UTILIZING ELECTRONIC MAIL

In accordance with the Federal Records Act and Army Regulation 25-1, Contractor personnel will use only Government-provided email services to conduct official Government business. Email services provided by a commercial service provider are prohibited for Army business communications containing sensitive information. Automatically forwarding from an official Government account to an unofficial (commercial service) is prohibited. There is no prohibition for manually forwarding email messages, one at a time, after opening and reading the content to ensure that the information is not sensitive or classified. All classified email communications will be conducted over the appropriately classified network.

When the Contractor personnel sends email messages to Government personnel using their Government provided email service while performing on this contract, the contract Contractor personnel's email addresses shall include "CTR" together with the person's name. All Contractor personnel shall ensure all emails include a signature block which identifies the individual sender as a Contractor employee to include company affiliation, the primary supporting Government office, and email and telephone contact information.

7.6 STANDARDS OF CONDUCT

The Contractor shall maintain satisfactory standards of employee competency and conduct, and for taking disciplinary actions against Contractor personnel as necessary. The Contractor shall remove from the job site any Contractor employee found under the influence of alcohol, illegal drugs, or any other incapacitating agent during the tour of duty.

The Contractor shall remove any employee whose conduct or appearance debases or discredits Agencies. The Government reserves the right to require removal from the job

site of any Contractor employee who endangers persons or property, whose continued employment is inconsistent with the interests of military security, or whose presence deters the accomplishment of required services. In such cases, the COR will advise the Contractor of the reason for requesting an employee's removal or withdrawal of his authorization to enter the installation.

The Government's exercise of its right to grant and revoke access by a particular individual(s) to its facilities will not constitute a breach or change to this PWS; regardless of whether said individual(s) is employed by the Contractor, and regardless of whether said individual(s) is thereby precluded from performing work under the PWS.

7.7 NONDISCLOSURE

The Contractor shall not divulge any information accessed and obtained during the course of performing this contract to other Contractor staff or anyone outside the Government. Specifically, in addition to any organizational conflict of interest provision, Contractor employees assigned to this contract shall be required, prior to working, to sign a nondisclosure statement for the Government agreeing not to share any information or data with other Contractor personnel not assigned to the project or, if assigned to the project, who has not signed a nondisclosure statement. Contractor employees who discuss Government business related to this contract to PL AESMS customers or non-customers may be removed for violating their Nondisclosure Agreement (NDA) and violating FAR Conflicts of Interest Clause 52.203-16 and Organizational and Consultant Conflicts of Interests Subpart 9.5.

Additionally, the Contractor shall not accrue or obtain any rights whatsoever in the data or information processed within the ETMS2 that is the subject of this contract. Such information and data are the exclusive property of the Agencies.

Uses and Safeguarding of Information- At no time shall any data be released to the public with the Contractor's name and contract number associated with the data.

7.8 INHERENTLY GOVERNMENTAL FUNCTIONS

The Contractor shall not perform any inherently governmental functions pursuant to FAR Part 7.500. The Contractor shall be required to perform the functions that are not considered to be inherently governmental functions, as set forth in FAR Part 7.503.

7.9 GOVERNMENT FURNISHED EQUIPMENT (GFE) AND INFORMATION

The Contractor employees assigned to organizational worksites shall have access to Government offices and equipment, such as computers, desks, and telephones, as necessary. The GFE shall be provided by the customer organization being supported. It is required that customer organizations provide GFE to the contractor employees for onsite work, and the GFE be capable of being used offsite in a telework status in the event of local, national or global crisis.

The Contractor shall be provided email, as well as other Government systems when required.

On-site Contractor personnel shall be in various Government facilities, both CONUS and OCONUS.

Contractor personnel shall have access only to those Government facilities, telephone, and computers necessary to execute the tasks of this contract and each customers' requirements.

The Contractor shall sign a hand receipt for all GFE. The Contractor shall account, be responsible for, and safeguard GFE in accordance with all DoD, branch/service, and organizational regulations and policies. This entails monitoring and safeguarding GFE from internal and external threats adhering to DoD Cyber Security Policies and Guidance.

7.10 OCONUS FACILITIES

Depending on the OCONUS location, the Government may provide access to DFAC, Exchange, and MWR facilities. Government office space may be provided to the Contractor based on post assignment. The Contractor shall be responsible for housing and transportation unless specified elsewhere in this PWS. All OCONUS provisions will be stipulated in each customers' requirements.

7.11 CONTRACTOR MANPOWER REPORTING

The Contractor shall comply with the following Contractor Manpower Reporting requirements:

The Contractor shall report ALL Contractor labor hours (including Subcontractor labor hours) required for the 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 following web address: https://www.sam.gov/SAM/.

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 NLT October 31 of each calendar year, beginning with 2021. The Contractors may direct questions to the help desk at: https://www.sam.gov/SAM/.

8. GOVERNMENT DATA RIGHTS

The Government has unlimited rights to all data, documents, and material produced under this contract in accordance with FAR Part 27.404-1. The Government has limited data rights to commercial computer software and commercial software documentation as determined by the FAR Part 27.404-2 and DFARS 227.7202-3. The Government's rights ~~will be~~are assigned in the Contractor's Software Licensing Agreement.

All materials, to include any data provided by the Government to establish the hosting and customer instances, 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 under the applicable Data Rights clause(s).

9. PRIVACY ACT

All contract personnel assigned to this contract shall have access to information that may be subject to the Privacy Act of 1974. The Contractor is responsible for ensuring all assigned contract personnel are briefed on the Privacy Act requirements.

10. CONTRACTING OFFICER REPRESENTATIVE (COR)

The COR will be identified by a separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions:

- Assure that the Contractor performs the technical requirements of the contract
- Perform inspections necessary in connection with contract performance
- Maintain written and oral communications with the Contractor concerning technical aspects of the contract
- Monitor the Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies
- Coordinate availability of Government furnished property, and provide or facilitate site entry of Contractor personnel.

A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates, or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

11. TRANSITION

The Contractor shall follow the phase-in plan, to be submitted NLT five (5) business days after award of the contract, and keep the Government fully informed of the status throughout the transition period. Throughout the phase-in/phase-out periods, it is essential that attention is given to minimize interruptions or delays to work in progress that would impact the mission.

The Contractor must plan for the deployment of their environment and migration of current customers, delineating the method for processing and assigning tasks during the migration periods. The transition for CONUS sites shall NOT exceed thirty (30) calendar days. The transition for OCONUS sites shall NOT exceed sixty (60) calendar days.

11.1 TRANSITION IN

Within five (5) business days after award of the contract, the Contractor shall submit a Phase-In plan that describes the details and schedule for providing an orderly transition during the contract's transition term. The Phase-In Plan will not be evaluated prior to the contract award. The Contractor shall provide a written response to the following:

- Identify the individuals responsible for facilitating a smooth transition.
- Identify all tasks that will be transitioned from the incumbent to the succeeding Contractor. The Contractor shall receive Government concurrence of any new or

changed management processes based on the Contractor's proposal. The COR will facilitate the transition of workload between the incumbent Contractor and the new Contractor.

- The incumbent and new Contractor are responsible for performing due diligence to ensure all transition activities are identified, negotiated, and completed during the transition term.
- Develop a resource-loaded project management schedule with measurable commitments. The activities performed during the transition term shall begin on the effective date of the contract award.
- Identify the time period for the project team to receive sufficient levels of enterprise training and familiarization to clearly understand all aspects of the project and accept full responsibility to provide in-house Contractor support to the Government client. The incumbent Contractor is responsible for all support service activities until the transfer of responsibilities is finalized to the Government's satisfaction.
- Complete transition-in by thirty (30) calendar days for CONUS support and sixty (60) calendar days for OCONUS support from contract award. The transition shall ensure minimum disruption to vital Government operations. The Contractor shall ensure there is no transition-related support issues degradation during the transition in.
- The final Transition-In Plan shall include:
    - A schedule with milestones, dates, and tasks
    - Description of activities to transition
    - Plan to transition knowledge and information from incumbent Contractor Key Personnel
    - Identification of potential risk management factors or problem areas and remediation/contingency operations plan

11.2 TRANSITION OUT

In the event the incumbent Contractor is not awarded the follow-on effort to this contract (ETMS2), there will be a maximum of thirty (30) calendar days allowed for any phase-out CONUS effort. However, for OCONUS support, the transition is sixty (60) calendar days for phase-out effort. During this period, the Contractor shall remain fully responsible for all efforts associated with the contract.

The Contractor shall agree to support the transition of work to another Contractor at the completion of the period of performance. The Contractor shall fully cooperate in providing all documentation to the incoming Contractor. The Contractor shall agree to migrate all government data into a hosting environment that is accessible to the government before the termination of this contract. If required, a joint inventory of any Government Furnished Property shall be conducted.

12. GOVERNMENT FURNISHED MATERIALS/FACILITIES

~~The~~With each customer's order, the Government will purchase, and the Contractor will install:

- Task Management Software Solution Software Licenses

- All software licenses necessary to support the backbone or architecture of the provided solution

13. DELIVERABLES AND MEETINGS

All deliverables are due by close-of-business (COB) of the scheduled date unless it falls on a holiday or weekend, at which point the deliverable is due the next business day. For the purposes of this contract, the COB is 4:00 p.m. Eastern Standard Time. The mode of delivery is electronic unless otherwise directed by the KO, or designated COR. The Contractor shall deliver as follows:

13.1 CONTRACT DELIVERABLES

13.1.1 PRICE WORKBOOK (CDRL A001)

The Contractor shall prepare a ~~Cost~~Price Workbook that is due with their proposal. The ~~Cost~~Price workbook shall include all line items separately priced by the number of users, with rates laid out for the base year and each option year. This will include labor rates by contractor duty position.

13.1.2 POST AWARD CONFERENCE / PERIODIC PROGRESS MEETINGS (CDRL A002)

The Contractor shall attend a post award conference convened by the contracting activity or contract administration office in accordance with FAR Subpart 42.5. The Contracting Officer, Contracting Officers Representative, and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings, the COR will apprise the Contractor of how the Government views the Contractor's performance, and the Contractor shall apprise the Government of problems, if any, being experienced. Appropriate action will be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government. The contractor shall provide any required briefing material ~~one (1) day~~two (2) business days prior to ~~the~~each scheduled meeting. This meeting may be conducted virtually or in-person.

13.1.3 PHASE-IN PLAN (CDRL A003)

The Contractor shall submit a Phase-In Plan, in writing, to the KO, or designated representative, not later than ~~five (5~~seven (7) days after contract award to describe how the Contractor will manage the transition and assumption of tasks and/or personnel and describes the details and schedule for providing an orderly transition during the contract's transition term. The PM shall be responsible for managing the plan. The plan is a working document and will be updated as required. When changes warrant, the updated plan shall be submitted to the KO or designated representative for approval within seven (7) days of the change.

13.1.4 PROGRAM MANAGEMENT AND SUPPORT PLAN (CDRL A004)

The Contractor shall submit a Program Management and Support Plan, in writing, to the KO, or designated representative, not later than fifteen (15) days of contract award to add

new Agencies organizations. The Management and Support Plan is a project management plan covering all task areas. The PM shall be responsible for managing the plan. The plan is a working document and will be updated as required. When changes warrant, the updated plan shall be submitted to the KO or designated representative for approval within seven (7) days of the change.

The Program Management and Support Plan shall detail the management, functional, and technical approach to support all elements of the contract for each task area. The plan shall include, but not limited to, organizational and equipment resources at the task area level, as well as management controls to be employed to meet the cost, performance, and schedule requirements throughout the contract execution.

The Program Management and Support Plan will also include the following sections at a minimum. These sections may be incorporated within the Management and Support Plan or delivered as stand-alone documents.

- Communication Management Plan
- Personnel Management Plan
- Risk Management Plan and Risk Matrix
- Issue Management Plan and Issue Matrix
- Security Management Plan
- Schedule Management Plan
- Sustainment Plan

Communications Management will include team member contacts and describe the communication methodology for project risks, issues and information.

Personnel Management shall describe how security clearance requirements are met, and detail the process to recruit and retain a qualified and capable workforce that can accomplish the entire scope of the efforts outlined in this PWS across multiple customer's requirements.

Risk Management will include a Risk Register that will be maintained throughout the life of the contract. Each risk will be documented and monitored through mitigation.

Issue Management will include an Issue Register that will be maintained throughout the life of the contract. Each risk and issue will be documented and monitored through resolution.

Security Management shall Standard Practice Procedure (SPP) which fully describes the security program, safeguards emergency procedures to be established to the protection of Government-furnished and contractor-developed classified materials prepared in conjunction with the project.

Schedule Management shall describe the practices for developing and progressing schedules for the contract and each customers' requirements.

Sustainment Plan shall describe the personnel responsible for and the processes for maintaining the environment for all customers.

13.1.5 MONTHLY PROGRESS REPORTS (CDRL A005)

A Monthly Progress Report shall be provided by the Contractor summarizing the overall project status. The report is due not later than the 10th workday of the following month. Delivery to the appointed representative from the AESMS program office by email is acceptable. This report shall summarize activities concluded during the previous month, taskers started, taskers completed, and other current status information. This monthly report shall be the primary management control process for the PWS. The Monthly Report shall contain the following:

- Brief description of requirements.
- Summary of accomplishments during the reporting period and significant events regarding the contract.
- Work Request status as defined by the COR.
- Deliverables submitted or progress on deliverable products.
- Any current or anticipated problems.
- Brief summary of activity planned for the next reporting period.
- Overall assessment of project glide path as dictated during the planning and analysis phase of the contract.
- Summary of help desk usage/phone support.

13.1.6 QUARTERLY IN PROGRESS REVIEW (CDRL A006)

The Contractor shall provide a quarterly In Progress Review (IPR) to The Contracting Officer, Contracting Officers Representative, and other Government personnel, as appropriate detailing progress of ETMS2 deployments, risks, issues and other pertinent data relevant to the cost, schedule and performance of the project(s). At these meetings, the COR will apprise the Contractor of how the Government views the Contractor's performance, and the Contractor shall apprise the Government of problems, if any, being experienced. Appropriate action will be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government. The contractor shall provide any required briefing material two (2) business days prior to each scheduled meeting. This meeting may be conducted virtually or in-person.

13.1.7 TECHNICAL INTERCHANGE MEETING (TIM) AGENDA AND MEETING MINUTES (CDRL A007)

The Contractor shall provide a monthly TIM agenda and meeting minutes. The function of this meeting is to provide an opportunity for the Government to discuss technical issues related to the hosting environment with the Contractor. The contractor shall support additional requirements as needed from the OSD and/or IT Reform Management Group. These meetings shall be at no additional cost to the Government. This meeting may be conducted virtually or in-person.

13.1.8 EXECUTIVE LEVEL PROJECT STATUS BRIEF (CDRL A008)

The Contractor shall provide an executive level project status brief upon request of the ~~Government or an ad hoc basis~~KO, COR or AESMS Program Management Office on an ad hoc basis. Briefings requested by customer's must be approved by the COR before scheduling. These meetings shall be at no additional cost to the Government. The contractor shall provide any required briefing material two (2) days prior to each scheduled meeting. This meeting may be conducted virtually or in-person.

13.1.9 SOFTWARE DATA RECOVERY PLAN (CDRL A009)

The Contractor shall provide a disaster recovery plan, within ninety (90) days of contract award, which outlines what the critical features of the procured task management software are and a detailed process on how to recover the task management software environment if a system restore is required.

The Contractor shall provide a quarterly upgrade and task management software support plan that outlines any weekly, monthly, and quarterly system checks.

13.1.10 HELP DESK SUPPORT OUTLINE (CDRL A010)

The Contractor shall provide an outline of the services that shall be provided by task management software Tier 2, and Tier 3 support desks, not later than ninety (90) days after contract award. The task management software support outline should identify POCs, hours of operation for each location, and ticket response times.

13.1.11 ARMY ENTERPRISE SERVICE DESK (AESD) KNOWLEDGE ARTICLES (CDRL A011)

The contractor shall provide AESD with Tier 0 and Tier 1 Knowledge Articles that will support the ETMS2 contract and the ETMS2 user community, not later than ninety (90) calendar days after contract award. Subsequent Knowledge Articles will be submitted within fourteen (14) calendar days after a Change Advisory Board (CAB) has convened and directed an update to the ETMS2 Knowledge Articles.

13.1.12 QUALITY CONTROL PLAN (CDRL A012)

The Contractor shall establish, within fifteen (15) days of contract award, and maintain a complete quality control program to assure the requirements of this contract are provided as specified. The Quality Control Plan will be delivered to the COR at the post award conference for approval. An updated copy shall be provided as changes occur.

As a minimum, the plan must include:

- A copy of the letter appointing the Contract Quality Control (CQC) representative, signed by an officer of the firm, outlining the CQC representative's duties, responsibilities, and authority.
- The quality control organization in chart form showing the relationship of the quality control organization to other elements of the firm.

- The names and responsibilities of personnel in the quality control organization involved with this contract.
- The area of responsibility and authority of each individual in the quality control organization.
- Contractor's procedures for reviewing all samples, certificates, or other submittal documentation for contract compliance.
- An inspection schedule, with a matrix keyed to each specific task, showing who will perform the work, who will inspect the work, and when the inspection will be performed. The schedule must specify areas to be inspected on both a scheduled or unscheduled basis and the titles of the individuals who shall do the inspection.
- The procedures for documenting quality control operation, inspection, and testing, with a copy of all forms and reports to be used for this purpose. The Contractor shall include a submittal status log listing all submittals required by the specifications and stating the action required by the Contractor or the Government. The Contractor shall complete the appropriate columns of the log and name the person(s) authorized to review the submittal.
- A method for identifying and correcting deficiencies and their causes in the quality of service performed before the level of performance is unacceptable.
- A file of all inspections conducted by the Contractor and the corrective action taken. This documentation shall be made available to the Government during the term of this contract.

13.1.13 OPSEC SOP/PLAN (CDRL A013)

The Contractor shall provide an OPSEC SOP/Plan, within ninety (90) days of contract award, which outlines the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it.

13.1.14 INSTALLATION GUIDE (CDRL A014)

The Contractor shall provide an installation guide not later than thirty (30) calendar days after contract award. The installation guide shall detail step-by-step instructions for deploying or installing the SaaS. A new copy will be delivered to the Government any time the guide is updated.

13.1.15 SYSTEM ADMINISTRATION GUIDE (CDRL A015)

The Contractor shall provide a system administration guide due not later than thirty (30) days after contract award. The system administration guide shall describe how to use the major features of the SaaS offering. A new copy will be delivered to the Government any time the guide is updated.

13.1.16 INFRASTRUCTURE DESIGN (CDRL A016)

The Contractor shall provide an architectural SaaS design that provides the capability to all Agency entities, due in five (5) business days prior to the Deployment Readiness Assessment.

13.1.17 DEPLOYMENT READINESS ASSESSMENT REPORT (CDRL A017)

The Contractor shall provide a Deployment Readiness Plan due ten (10) days from the end of the assessment beginning of the period of performance (PoP) after contract award. The assessment will include the findings from the technical and functional assessment of Agencies' readiness.

13.1.18 PHASE-OUT TRANSITION PLAN (CDRL A018)

The Contractor shall submit a Phase-Out Transition Plan, in writing, to the KO, or designated representative, not later than ninety (90) days before the end of the period of performance. The Phase-Out Transition Plan will describe how the Contractor will manage the transition of tasks and/or personnel and describes the details and schedule for providing an orderly transition off of the project. The PM shall be responsible for managing the plan. The plan is a working document and will be updated as required. When changes warrant, the updated plan shall be submitted to the KO or designated representative for approval within seven (7) days of the change.

13.2 CUSTOMER REQUIREMENTS DELIVERABLES

13.2.1 POST AWARD CONFERENCE / PERIODIC PROGRESS MEETINGS (CDRL B001)

The Contractor shall attend a post award conference at the beginning of each customers' period of performance convened by the contracting activity or contract administration office in accordance with FAR Subpart 42.5. The Contracting Officer, Contracting Officers Representative, and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings, the COR will apprise the Contractor of how the Government views the Contractor's performance, and the Contractor shall apprise the Government of problems, if any, being experienced. Appropriate action will be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government. The contractor shall provide any required briefing material two (2) business days prior to each scheduled meeting. This meeting may be conducted virtually or in-person subject to the specific customer's requirements.

13.2.2 PERIODIC STATUS REPORTS (CDRL B002)

A Periodic Status Report shall be provided by the Contractor summarizing the individual customer's implementation progress. The report is due NLT Tuesday following the prior period beginning with the first full work week after the customers' post award conference. Delivery to the organizational POC and appointed representative from the AESMS program office by email is acceptable. The report will be delivered on a weekly basis at the beginning of the customer's period of performance but can be adjusted to biweekly or monthly based on the desires of the organization. This report shall summarize activities concluded during the previous week, taskers started, taskers completed, and other current status information. This monthly report shall be the primary management control process for the PWS. The Weekly/Biweekly/Monthly Report shall contain the following:

- Brief description of requirements.

- Summary of accomplishments during the reporting period and significant events regarding the contract.
- Work Request status as defined by the COR.
- Deliverables submitted or progress on deliverable products.
- Any current or anticipated problems.
- Brief summary of the activity planned for the next reporting period.
- Overall assessment of project glide path as dictated during the planning and analysis phase of the contract.
- Summary of Help Desk usage/phone support.

13.2.3 PERIODIC STATUS MEETING AGENDA AND MEETING MINUTES (CDRL B003)

The Contractor shall provide a Periodic Status Meeting agenda and meeting minutes. The function of this meeting is to provide an opportunity for the Government organization to discuss the status and progress of implementation and sustainment related topics with the Contractor. The meeting will be scheduled as a weekly meeting at the beginning of each customers' period of performance can be adjusted to biweekly or monthly based on the desires of the organization. Delivery to the organizational POC and appointed representative from the AESMS program office by email is acceptable. This meeting may be conducted virtually or in-person subject to the specific customer's requirements.

13.2.4 PROJECT PLAN (CDRL B004)

The Contractor shall provide a detailed project plan NLT thirty (30) days after each customers' period of performance begins. The project plan shall provide specific (to the calendar day) anticipated start and finish points for each project phase. The project plan shall include anticipated resources required by or from the Government, for execution of each phase. The project plan shall include a quantifiable desired end state for each phase. The project plan shall document the organization and personnel responsible for sustaining and supporting the ETMS2 products and user community during and after implementation. The Contractor shall provide an MS Project 2013 compatible schedule that incorporates both Contractor tasks, as well as required Government tasks.

13.2.5 STRATEGIC COMMUNICATION PLAN (CDRL B005)

The Contractor shall provide a strategic communication plan due ten (10) days after the start of each customers' period of performance. The strategic communication plan shall provide the communication strategy, marketing information to Agencies, users, and messaging from senior leaders. The Contractor provides the document template, and the Government will create the document.

13.2.6 TRAINING PLAN (CDRL B006)

The Contractor shall provide a training plan due fifteen (15) calendar days after the start of each customers' period of performance. The training plan shall provide documentation on how the user community will be trained on the ETMS2. It includes training best

practices, schedule and logistics, and training numbers to support user deployment checklist.

13.2.7 EXECUTIVE LEVEL PROJECT STATUS BRIEF(CDRL B007)

The Contractor shall provide an executive level project status brief upon request of the ~~Government or an ad hoc basis.~~KO, COR or AESMS Program Management Office on an ad hoc basis. Briefings requested by customer's must be approved by the COR before scheduling. These meetings shall be at no additional cost to the Government. The contractor shall provide any required briefing material two (2) days prior to each scheduled meeting. This meeting may be conducted virtually or in-person subject to the specific customer's requirements.

14. QUALITY ASSURANCE

The Contractor shall meet performance standards listed in this PWS; and shall not be relieved of any performance requirements due to a delay in the delivery of supplies, materials, parts, or a lack of personnel support.

The Government will evaluate the Contractor's performance using the Quality Assurance Surveillance Plan, as outlined in paragraph 14.2 this PWS.

14.1 MILESTONES

For each customers' order, ~~T~~the Contractor shall meet the milestones listed below, and any others identified in each customers' requirements, in order to ensure the contract remains on schedule with appropriate time allocated to address issues.

- The Contractor shall create the organizational instance with a distinct URL, install their ETMS2, and any ancillary software necessary to operate the SaaS onto servers NIPR & SIPR hosting environments NLT fifteen (15) calendar days after the start of each customers' period of performance.
- The Contractor shall deploy the NIPR/SIPR instance of the system and complete training of the workforce for each customer's order within the specified number of weeks, as reflected in Table 1. Training will be conducted in the most economical manner possible to include exploiting opportunities for using web-based or computer-based training, and implementing Train-the-Trainer programs within each customer's organization.
- IOC is achieved once the Contractor has prepared the organizational tasking structure, established the necessary interorganizational connections to CATMS, TMT, and/or other instances of the ETMS2, developed initial workflows within the ETMS2, trained the applicable percentage of total licensed users, and conducted a Validation Exercise. The timeframe and percentage of users that must be trained to successfully meet IOC for each customer's order is detailed in Table 1.
- Full Operating Capability (FOC) is achieved when all licensed users have been trained and the organization has met all "Go-Live" requirements. The timeframe to achieve FOC for each customer's order is detailed in Table 1.

Number of Users	IOC		FOC
	Percentage of Users	Timeframe	Timeframe
1-200	15%	6 weeks	12 weeks
201-400	15%	8 weeks	16 weeks
401-600	20%	10 weeks	21 weeks
601-800	20%	12 weeks	25 weeks
801-1000	30%	15 weeks	30 weeks
1001-1200	30%	17 weeks	35 weeks
1201-1400	30%	19 weeks	39 weeks
1401-1600	40%	22 weeks	44 weeks
1601-1800	40%	24 weeks	48 weeks
1801-5000	50%	26 weeks	52 weeks
5000-10000	50%	39 weeks	78 weeks

Table 1 ETMS2 Training Milestones

14.2 PERFORMANCE REQUIREMENTS SUMMARY (PRS)

The Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #1 The Contractor shall provide a Price Workbook **PWS Paragraph** 13.1.1	Documents the cost of licenses and services related to the Software-as-a-Service priced by tiers of numbered users with rates for each contract year. Deliverable to the COR via email.	Deliver during the post award conference, but NLT thirty (30) days after contract award	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established standard from Acceptable Quality Level (AQL) may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative Contractor Performance Assessment Reporting System (CPARS) report
PRS #2 The Contractor shall attend a Post Award Conference /Periodic Progress Meetings **PWS Paragraph** 13.1.2 **PWS Paragraph** 13.2.1	Provides briefing material for the meeting Deliverable to the COR via email. Presented in-person/virtually to designated recipients	Deliver one (1) day prior to the post award conference or meeting	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #3 The Contractor shall provide a Phase-In Plan **PWS Paragraph** 13.1.3	MS Word document detailing phase-in efforts. MS Project 2013 Schedule with integrated work breakdown structure. Deliverable to the COR via email.	NLT the five (5) days after contract award.	Contracting Officer's Representative Review 100% Inspection	Failure to comply with established Performance Objective over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #4 The Contractor shall provide a Program Management and Support Plan **PWS Paragraph** 13.1.4	Documents how security clearance requirements are met, and detail the process to recruit and retain a qualified and capable workforce. Deliverable to the COR via email.	Deliver during the post award conference, but NLT fifteen (15) days after contract award. Updates provided with seven (7) days of request.	COR Review 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #5 The Contractor shall provide a Monthly Progress Report **PWS Paragraph** 13.1.5	MS Word document detailing rollup of weekly reports. Deliverable to the COR via email.	Report received by the COR not later than the 10th working day of the following month	COR Review 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #6 The Contractor shall provide an ~~in-progress review~~In-Progress Review **PWS Paragraph** 13.1.6	Quarterly. Deliverable to the COR via email. Presented in-person/virtually to designated recipients	Report received by the COR NLT the first Monday of each fiscal quarter (OCT, JAN, APR, JUL)	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #7 The Contractor shall provide a TIM Agenda & Meeting ~~minutes~~Minutes **PWS Paragraph** 13.1.7	Monthly TIM agenda & meeting minutes. Deliverable to the COR via email.	Report received by the COR NLT the 10th working day of the following month	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #8 Executive Level Project Status Brief **PWS Paragraph** 13.1.8 **PWS Paragraph** 13.2.7	Ad hoc. Deliverable to the COR via email for read-ahead. Presented in-person/virtually to designated recipients	Briefing material delivered to the COR two (2) days prior to the requested meeting. Brief presented to GO/SES level upon request	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #9 The Contractor shall provide a Software Data Recovery Plan **PWS Paragraph** 13.1.9	Documents the process on how to recover the task management software environment if a system restore is required. Deliverable to the COR via email.	Draft: Thirty (30) days after contract award. Final: Ninety (90) days after contract award.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #10 The Contractor shall provide a Help Desk support Outline **PWS Paragraph** 13.1.10	Documents the services provided for Tier 2 & 3 Help Desk Support. Deliverable to the COR via email.	Draft: Thirty (30) days after contract award. Final: Ninety (90) days after contract award.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #11 The Contractor shall provide AESD Knowledge Articles **PWS Paragraph** 13.1.11	Provides AESD with Knowledge Articles to support providing ETMS2 users with Tier 0 and Tier 1 Help Desk Support. Deliverable to the COR via email.	Initial: Ninety (90) days after contract award. Updates: Fourteen (14) days after requested by Change Advisory Board (CAB).	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #12 The Contractor shall provide a Quality Control Plan **PWS Paragraph** 13.1.12	Documents the Contractor's Quality Control Measures to ensure contract requirements are provided as specified. Deliverable to the COR via email.	Not later than fifteen (15) days after contract award.	Government provides input, review and accepts. COR reviews. 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #13 The Contractor shall provide an Operational Security Standard Operating Procedure or Plan, **PWS Paragraph** 13.1.13	Documents the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. Deliverable to the COR via email	Not Later than ninety (90) days after contract award.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #14 The Contractor shall provide an Installation Guide, **PWS Paragraph** 13.1.14	Documents step-by-step instructions for deploying or installing the SaaS offering. Deliverable to the COR via email	Not Later than thirty (30) days after contract award.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #15 The Contractor shall provide a System Administration Guide **PWS Paragraph** 13.1.15	Documents how to use the major features of the SaaS offering. Deliverable to the COR via email.	NLT the thirty (30) days after contract award.	Government reviews and accepts. 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #16 The Contractor shall provide an Infrastructure Design. **PWS Paragraph** 13.1.16	Customer provides network diagrams, Integrator updates to reflect where the SaaS offering fits. Deliverable to the COR via email	Not later than five (5) days after completing Deployment Readiness Assessment	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #17 The Contractor shall provide a Deployment Readiness Assessment Report **PWS Paragraph** 13.1.17	Details the findings from technical and functional discovery and assessment of customer readiness. Deliverable to the COR via email	Not Later than ten (10) days after completing Deployment Readiness Assessment	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #18 The Contractor shall provide a Phase-Out Plan **PWS Paragraph** 13.1.18	MS Word document detailing phase-out efforts. MS Project 2013 Schedule with integrated work breakdown structure.	Not Later than ninety (90) days before the end of the period of performance.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #19 The Contractor shall provide a Periodic Progress Report **PWS Paragraph** 13.2.2	MS Word document detailing the past periods activities. Deliverable to the Lead Organizational POC and COR.	First 2 Months: Due weekly, NLT the Tuesday following the previous week Subsequent Months: Biweekly or Monthly based on agreed timeframe with AESMS and supported organization(s, due the Tuesday following the previous period	COR reviews 100% Inspection	Failure to comply with established Performance Objective over and above the established Standard from Acceptable Quality Level (AQL) may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #20 The Contractor shall provide a Periodic Status Meeting Agenda & Meeting Minutes **PWS Paragraph** 13.2.3	Agenda: MS Word document outlining topics to be discussed Minutes: MS Word Document detailing • The names of the participants • Agenda items • Calendar or due dates • Actions or tasks • Decisions made by the participants • Record of the conversation • Future decisions Deliverable to the Lead Organizational POC and COR.	Deliverable to the Lead Organizational POC and COR Agenda: Deliverable to the not later than 24 hours prior to meeting start Minutes: Due NLT 48 hours after meeting conclusion.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #21 The Contractor shall provide a Project Plan **PWS Paragraph** 13.2.4	MS Word document documenting quantifiable desired end state for each phase and MS Project 2013 Schedule with integrated work breakdown structure. Deliverable to the Lead Organizational POC and COR.	Due not later than thirty (30) days after the start of each customers' period of performance.	Government provides input, review and accepts. COR reviews. 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #22 The Contractor shall provide a Strategic Communication Plan **PWS Paragraph** 13.2.5	Includes communication strategy, marketing information to users, and messaging from Sr. leaders. Deliverable to the Lead Organizational POC and COR.	Contractor will provide a document template and input to each customer. Government will create the document.	Government accepts document template and input. 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #23 The Contractor shall provide a Training Plan **PWS Paragraph** 13.2.6	Documents how the user community will be trained on the Task Management Software; includes training best practices, schedule, and logistics includes training numbers to support user deployment checklist. Deliverable to the Lead Organizational POC and COR via email	Due not later than fifteen (15) days after the start of each customers' period of performance.	Government provides input, review and accepts. 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #24 The Contractor shall deploy or install the SaaS for new organizations. **PWS Paragraph** 4.1 **PWS Paragraph** 14.1	Deploy custom URL and install all necessary software on both NIPRNet and SIPRNet.	New instances of the SaaS offering will be operational not later than 15 days after the start of each customers' period of performance.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #25 The Contractor shall configure the SaaS offering for new customers. **PWS Paragraph** 4.1	SaaS offering will be configured according to each organization's hierarchy and task management processes.	100% of configuration completed by each customers' IOC.	Government provides input, review and accepts. 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #26 The Contractor shall provide Tier 3 Help Desk Support for all organizations **PWS Paragraph** 4.3	Tier 3 Help Desk support will be available to all organizations during each organizations' normal business hours.	90% of help desk tickets solved within 24 hours of receipt.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #27 The Contractor shall provide training for new organizations task management personnel. **PWS Paragraph** 4.4 **PWS Paragraph** 14.1	Provide user level specific training.	90% of licensed users trained by each customers' FOC.	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Performance Objective (Task / Deliverable)	Standard	Performance Threshold (This is the maximum error rate)	Method of Surveillance	Remedies
PRS #28 The Contractor shall achieve IOC for all new organizations. **PWS Paragraph** 14.1	Conduct all training, configurations and validation exercises within the timeframes specified within Table 1 for the organizations specified number of users.	No more than 10% schedule delay not including Government caused delays	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report
PRS #29 The Contractor shall achieve FOC for all new organizations. **PWS Paragraph** 14.1	Conduct all training, configurations and validation exercises within the timeframes specified within Table 1 for the organizations specified number of users.	No more than 10% schedule delay not including Government caused delays	COR reviews 100% Inspection	Failure to comply with established Performance Objectives over and above the established Standard from AQL may result in reduction of payment equal to the applicable labor rate times the number of hours of services that were not provided. Negative CPARS report

Table 2 Performance Requirements Summary

15. APPLICABLE PUBLICATIONS, REGULATIONS, DIRECTIVES, POLICIES (CURRENT EDITIONS)

The Contractor shall abide by all applicable regulations, publications, manuals, and local policies and procedures.

- Joint Travel Regulations (JTR)
- Army Regulation 25–1, "Army Information Technology" dated June 25, 2013
- Army Regulation 25–2, "Information Assurance" dated October 24, 2007; Rapid Action Revision (RAR), Issue Date: March 23, 2009
- Army Regulation 380–5, "Department of the Army Information Security Program" dated September 29, 2000
- Army Regulation 380–49, "Industrial Security Program" dated March 20, 2013
- Army Regulation 380–53 "Communications Security Monitoring" dated January 23, 2012
- Army Regulation 380–67, "Personnel Security Program" dated January 24, 2014
- Army Regulation 500–3, "U.S. Army Continuity of Operations Program Policy and Planning" dated April 18, 2008
- Army Regulation 530–1, "Operations Security " dated September 26, 2014
- Army Regulation 700-142, Type Classification, Materiel Release, Fielding and Transfer dated June 2, 2015
- Army Regulation 735-5, Property Accountability Policies dated August 22, 2013
- Army Regulation 735-11-2, Reporting of Supply Discrepancies dated 6 August 2001
- CJCS Instruction 6510.01F, "Information Assurance (IA) and Computer Network Defense (CND)" dated 9 February 2011
- Computer Security Act of 1987 (Public Law No. 100-235 (H.R. 145)) dated January 8, 1988
- DCI Directive 6/3, “Protecting Sensitive Compartmented Information within Information Systems” dated June 5, 1999
- DCI Directive 6/4, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)” dated July 2, 1998
- DCI Directive 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities” dated November 18, 2002
- Defense Acquisition Guidebook – Chapter 7, “Acquiring Information Technology” dated December 8, 2008
- Defense Information Systems Agency (DISA) IAVM Process Handbook, Ver. 3, dated February 2007
- Department of the Army Pamphlet 25–1–1, "Army Information Technology Implementation Instructions " dated September 26, 2014
- Department of the Army Pamphlet 25–1–2, "Information Technology Contingency Planning" dated June 6, 2012
- DoD 5200.2-R, “Personnel Security Program” dated January 1987 (Administrative Reissuance Incorporating through Change 3, February 23, 1996)

- DoD 5400.11-R, “Department of Defense Privacy Program” dated May 14, 2007
- DoD 6025.18-R “DoD Health Information Privacy Regulation” dated January 24, 2003
- DoD CIO Memo "Certification and Accreditation Requirements for DoD Managed Enterprise Services Procurements" dated June 22, 2006
- DoD Information Assurance Vulnerability Alert (IAVA) memorandum dated December 30, 1999
- DoD Directive 3020.26, " Defense Continuity Programs (DCO)" dated January 9, 2009
- DoD Directive 5400.11, “DoD Privacy Program” dated October 29, 2014
- DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)" dated March 17, 2016
- DoD Directive 8140.01, “Cyberspace Workforce Management” dated August 11, 2015
- DoD Directive 8320.02, “Data Sharing in a Net-Centric Department of Defense” dated December 2, 2004 – Certified Current as of April 23, 2007
- DoD Directive 8500.01E, "Information Assurance” dated October 24, 2002; Certified Current as of April 23, 2007
- DoD Instruction 3020.37, "Continuation of Essential DoD Contractor Services During Crises" dated November 6, 1990, Administrative Reissuance Incorporating Change 1, January 26, 1996
- DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)" December 30, 1997
- DoD Instruction 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance” dated July 14, 2015
- DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology dated March 12, 2014
- DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System" dated July 9, 2004
- DoD Instruction 8910.01 “Information Collecting and Reporting” dated May 19, 2014
- DoD IPv6 Standard Profiles for IPv6 Capable Products Version 6.0 dated July 2011
- DoD Manual 5220.22-M "National Industrial Security Program Operating Manual (NISPOM)” dated February 28, 2006
- DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program " dated 19 December, 2005 - Incorporating Change 4, dated November 10, 2015
- DoD Memorandum "Disposition of Unclassified DoD Computer Hard Drives" dated June 4, 2001
- E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. §101, H.R. 2458/S. 803) enacted on December 17, 2002, with an effective date for most provisions of April 17, 2002

- Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules” dated May 25, 2001 and revised December 3, 2002
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) dated January 2008 (WH release on Comprehensive National Cybersecurity Initiative, March 2, 2010)
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "Revised Fact Sheet National Information Assurance Acquisition Policy" and associated "Frequently Asked Questions" dated January 2000, and revised July 2003
- NIST Special Publication 800-53 Revision 4, " Security and Privacy Controls for Federal Information Systems and Organizations" dated April 2013
- OMB Circular A-130 (57 FR 18296) dated April 29, 1992 (Transmittal No. 4 dated November 28, 2000)
- The National Security Act of 1947 (Pub. L, No. 235, 80 Cong., 61 Stat. 496, 50 U.S.C. Ch 15) dated July 26, 1947
- Section 3541 of title 44, United States Code, “Federal Information Security Management Act of 2002” (FISMA)Strategic Command Directive (SCD) 527-1, “Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures” dated 27 January 2006
- Public Law 107-347, 44 U.S.C. § 101; E-Government Act of 2002, Title III: Information Security (Federal Information Security Management Act of 2002 (FISMA)) dated December 17, 2002
- The Privacy Act of 1974, 5 U.S.C. § 552v (2015 Edition)
- Clinger Cohen Act of 1996, Title 40 (Pub L. 104-106, Division E) dated February 10, 1996

Section 508

- Section 508. https://www.section508.gov/
- Section 508 – Electronic and Information Technology. 21 December 2000, https://www.justice.gov/sites/default/files/crt/legacy/2009/02/18/508law.pdf
- Desktop and Portable Computer (1194.26)

DoD and Army Documents

- Joint CONOPS Concept of Operations for Global Information Grid - Army, NETOPS CONOPS
- Defense Information Infrastructure Master Plan, Version 7.0
- Deputy Under Secretary of Defense (Logistics and Materiel Readiness) Logistics Enterprise Integration and Transformation https://www.acq.osd.mil/log/logistics_materiel_readiness/organizations/lsm/assetts/feb_02_information/ei_info/pdfs/Ent%20Integ%20and%20Transformation%20Dec%2001.pdf
- DISA Policy on Network Communications http://www.fas.org/nuke/guide/usa/doctri%20ne/DoD/DoDd-4660_3.htm

Records Management

- DoD Electronic Records Management Software Applications Design Criteria Standard

Other Regulatory and Commercial Requirements

- Distributed Management Task Force Desktop Management Interface (DMI) Version 2.0 https://www.dmtf.org/standards/dmi
- Security Requirements for Cryptographic Modules https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf
- Latest Windows 2000 and Windows NT Hardware Compatibility List ftp://ftp.microsoft.com/services/whql/hcl/wi%20n2000hcl.txt

DoD Level Policy References

- DoD Instruction 8510.01
- Compliance with DoD Web Site Administration Policy, https://www.dodig.mil/Audit/reports/fy01/01-130.pdf, http://www.dodig.mil/Audit/reports/fy01/01-130.pdfMay 31, 2001
- Destruction of DoD Computer Hard Drives Prior to Disposal Memorandum by Deputy Secretary of Defense, https://iase.disa.mil/policy-guidance/destruction-of-DoD-computer-hard-drives-prior-to-disposal-01-08-01.pdf, Jan 8, 2001
- Signed DoD Memorandum - Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, https://iase.disa.mil/policy-guidance/DoD-dar-tpm-decree07-03-07.pdf, Jul 03, 2007
- Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media Memo, https://iase.disa.mil/policy-guidance/faq_dar_encryption_policy_memo_18mar08_update-6_final.doc, Mar 19, 2008
- DoD IT Standards Registry (DISR)
- DoD Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement, https://iase.disa.mil/policy-guidance/DoD-banner-9may2008-ocr.pdf, May 9, 2008
- DoD Telework Policy, http://www.dtic.mil/whs/directives/corres/pdf/103501p.pdf, Oct 21, 2010
- DoD Web and Internet-based Capabilities (IbC) Policies, http://www.defenselink.mil/webmastershttp://www.defenselink.mil/webmasters
- DoD Web Site Administration Policies and Procedures (with amendments), http://www.defenselink.mil/webmasters/policy/DoD_web_policy_12071998_with_amendments_and_corrections.html, Jan 11, 2002
- IA Section of the Draft Defense Acquisition Guidebook, http://iase.disa.mil/policy-guidance/ia-section-of-draft-defense-acquisition-guidebook.doc, Jul 9, 2004
- Open Source Software in the Department of Defense (DoD) Memorandum, M http://cio-nii.defense.gov/sites/oss/2009OSS.pdf, May 28, 2003

- Web site OPSEC Discrepancies
http://www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DoD_webmasters.html, Jan 14, 2003
- Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) Certified Current April 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf, May 5, 2004
- Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf, June 30, 2004
- Electronic Newspaper Policy, http://www.defenselink.mil/webmasters/policy/5120_4.html, May 29, 1996
- Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) Directive Cancels DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))"
- DoD Directive 5215.1 Computer Security Evaluation Center, https://hsdl.org/?view&doc=1833&coll=limited, Oct 25, 1982
- Global Information Grid Overarching Policy, http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf, Feb 10, 2009
- DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) Certified Current April 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf, Apr 14, 2004
- Information Technology Portfolio Management, http://www.dtic.mil/whs/directives/corres/pdf/811501p.pdf, Oct 10, 2005
- Information Assurance (IA) Implementation. http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf,DoD Instruction 8500.2, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf, Feb 6, 2003
- DoD Directive 8520.1, Protection of Sensitive Compartmented Information (SCI) June 13, 2011 http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf
- DoD Directive O-8530.1 – Computer Network Defense (CND)
- DoD Instruction O-8530.2 – Support to Computer Network Defense (CND)
- DoD Directive 8530.1-M – Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process
- Ports, Protocols, and Services Management (PPSM), http://iase.disa.mil/ports/index.html, Aug 13, 2004

Department of the Army Policy References

- http://www.usapa.army.mil/pdffiles/r70_1.pdfArmy Acquisition Policy, http://www.usapa.army.mil/pdffiles/r70_1.pdf, Dec 31, 2003

Army Enterprise Standardization

- Army Enterprise Desktop Software Standardization (TECHCON 2004- 005b). 5 Nov 2004.

- Memorandum Establishing Army MS ELA Software Inventory as Single Source for Obtaining MS Products. 04 February 2004
- Moratorium on Microsoft Products and Product Support Services, https://chess.army.mil/ascp/commerce/scp/downloads/contracts/aei-esc_ms/Moratorium_ltr.pdf, 19 June 2003

Risk Management Framework (RMF)

- DoDI 8510.01 "Risk Management Framework for DoD Information Technology" – 24 May 2016
- Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM) – 4 Jun 2018
- NIST Special Publication 800-37 Risk Management Framework for Information Systems and Organization – Oct 2018 (Draft)
- NIST Special Publication (SP) 800-37 (Rev. 1)
- Federal Information Processing Standard (FIPS) Publication 199 and NIST SP 800-60 vol. 1 , NIST SP 800-60 vol. 2
- FIPS 200 and NIST SP 800-53 (Rev. 4)
- NIST SP 800-53A (Rev. 1)
- NIST SP 800-137
- NIST SP 800-59
- CNSS Publication (CNSSP) 22
- CNSS Instruction (CNSSI) 1253
- CNSS Instruction (CNSSI) 1254

DoD Information Technology Standards Registry

- DoD Information Technology Standards Registry Baseline Release 04-2.0. 22 December 2004
- DoD Information Technology Standards Registry (Note: Access to the DISR requires registration/login to the DISA DISR online website)
- Applicable mandatory standards in DISR shall be implemented by the Contractor

System Security

- CJCSM 3170.01B: Operation of the Joint Capabilities Integration and Development System. http://www.dtic.mil/cjcs_directives/cdata/unlimit/m317001.pdf

Data Collection and Retention

- Freedom of Information Act
  - DoD Directive 5400.7, Change 1, of 4/11/2006
  - Freedom of Information Act, Chapters 2-8
  - The Freedom of Information Act, U.S.C. Section 552, as amended by P.L. No. 104-231, 110 Stat 3048, (1996)
- The Privacy Act of 1974, amended, 2004, 5 USC Section 552a

Appendix A GENERAL REPORTS

- General Suspense
- General Suspense Master Control Comments
- General Suspense Master Control and Tasking Remarks
- External Suspense
- General Suspense With Special Items
- General Suspense With Interim Date
- General Suspense With Partial Remarks
- General Suspense With Full Remarks
- General Suspense With Constituents
- Originator General Suspense
- Office of Secretary Defense (OSD) Items
- Taskers
- Normal
- Red Top
- CSA Directed
- VCSA Directed
- Organization initiated
- SAAL General Suspense
- Due in 2 days
- Due in 7 days
- Overdue
    - Over 60 days
    - 31-60 Days
    - 16-30 Days
    - 1-15 Days
- Digest Report
- Log Report
- SAAL Tasker Summary
- Users List
- Special Items
- Keyword
- Open Daily
- Batch Tasker
- Cases Entered
- Master Control Information
- Task / Image Audit
- Work Production
- Production Summary
- Office of General Counsel (OGC) Freedom of Information Act (FOIA) Summary
- OGC FOIA Details

- FOIA Summary / Annual
- Monthly Taskers
- User Reports
- Rejected Tasker Summary
- Rejected Tasker Details
- Organizational Performance Metrics – percentage or count of accepted, rejected, reworked tasks, etc.

Appendix B SPECIAL REPORTS

- Open Cases
- Open Cases (Telephone)
- Open Cases (All)
- Signature
- Production
- Subject Analysis
- State/Congress
- Management
- Batch
- Congressional Leadership
- Flagged Cases
- OSD Suspense
- Input Source Codes
- Subject Codes
- Master Control Lookup

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix C SUSPENSE REPORTS

- Due within a date range
- Type of action
- Entire organization
- By action officer(s)
- By tasking official(s)
- Choice of sort options
- Control number
- Suspense date
- Action officer
- Originator
- Organization
- Type of action
- Type of action by agency

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix D WORKLOAD STATISTICAL REPORTS

The user must specify the reporting period for the date to be selected for these reports. All taskers that were received, closed, open, or overdue within the reporting period will be selected. The following reports allow the user to view and examine statistics with regards to production detail and summary information as well as to track case workloads:

- Due in 2 days
- Due in 7 days
- Overdue
- Digest Report
- Log Report
- SAAL Tasker Summary
- Users List
- Special Items
- Keyword
- Open Daily
- Batch Tasker
- Cases Entered
- Master Control Information
- Task / Image Audit
- Work Production
- Production Summary
- OGC FOIA Summary
- OGC FOIA Details
- FOIA Summary / Annual
- Number of taskers assigned to principal organization by week/month/year
- Number of taskers completed by principal organization by week/month/year
- Average days to complete action by principal organization
- Number of taskers returned to principal organization by week/month/year
- Reason code for taskers returned to principal organization for correction by week/month/year
- Average number of taskers returned to principal organization by week/month/year

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix E DEFINITIONS

CONTRACTOR A supplier or vendor having a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

CONTRACTING OFFICER A person with authority to enter into, administer, and or terminate contracts and make related determinations and findings on behalf of the Government. Note: The only individual who can legally bind the Government.

CONTRACTING OFFICER'S REPRESENTATIVE (COR) An employee of the USG appointed by the contracting officer to administer the contract. Such appointment will be in writing and will state the scope of authority and limitations. This individual has authority to provide technical assistance to the Contractor as long as that assistance is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

CUSTOMER(S) Individual organizations that procure ETMS2 through the PL AESMS program management office. Customers may have unique requirements for the individual deployment and configuration of their instance of ETMS2 within the overall AESMS environment.

DAYS In relation to due dates, deadlines and suspenses, for the purposes of this contract the term a number of days refers to “calendar days” unless otherwise specified. Wherever “working days” or “business days” days are specified, the holidays recognized in paragraph 3.4 are excluded from the count.

DEFECTIVE SERVICE A service output that does not meet the standard of performance associated with the PWS.

DELIVERABLE Anything that can be physically delivered but may include non-physical things such as meeting minutes.

FULL OPERATING CAPABILITY The state achieved when the ETMS2 is delivered to an organization, and they have the ability to fully employ and maintain it to meet the operational need.

INITIAL OPERATING CAPABILITY The state achieved when the ETMS2 is considered to be in its minimum usefully deployable form for an organization.

LOCAL STANDARD TIME The clock time for the time zone in which the observing site is situated, but which does not include any shift in time due to the implementation of daylight saving time.

QUALITY CONTROL All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

SUBCONTRACTOR One that enters into a contract with a Prime Contractor. The Government does not have privet of contract with the Subcontractor.

WORK DAY The number of hours per day the Contractor provides services in accordance with the contract.

WORK WEEK Defined as Monday through Friday unless specified otherwise.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix F ACRONYMS

AESD	Army Enterprise Service Desk
AO	Action Officer
AOR	Area of Responsibility
APACS	Aircraft and Personnel Automated Clearance System
APL	Approved Products List
AQL	Acceptable Quality Level
AR	Army Regulation
ASSA	Analytical Support Accreditation
AT	Antiterrorism
ATCTS	Army Training Certification Tracking System
ATO	Authority to Operate
CAB	Change Advisory Board
CAC	Common Access Car
CACO	Congressional Action Control Officer
CATMS	Correspondence and Task Management System
CBT	Computer Based Training
CDRL	Contract Data Requirements List
CLIN	Contract Line Item Number
COB	Close of Business
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Officer’s Representative
COTS	Commercial-Off-the-Shelf

CPARS	Contractor Performance Assessment Reporting System
CQC	Contract Quality Control
CRC	CONUS Replacement Center
CTR	Contractor
DA	Department of the Army
DCOPS	DOCPER Contractor Online Processing System
DD250	DoD Form 250 (Receiving Report)
DD254	DoD Contract Security Requirement List
DFARS	Defense Federal Acquisition Regulation Supplement
DII	Defense Information Infrastructure
DOCPER	DOD Contractor Personnel Office
DoD	Department of Defense
DSSR	DoD Standardized Regulations
ETMS2	Enterprise Task Management Software Solution
FAR	Federal Acquisition Regulation
FFP	Firm Fixed Price
FOC	Full Operational Capability
FOIA	Freedom of Information Act
FPCON	Force Protection Condition
FTR	Federal Travel Regulations
FY	Fiscal Year
GAL	Global Address List
GFE	Government Furnished Equipment
HIPAA	Health Insurance Portability and Accountability Act of 1996
HPCON	Health Protection Condition
IA	Information Assurance

IAW	In accordance with
IAVA	Information Assurance Vulnerability Alert
IC	Invited Contractors
ID	Identification
IOC	Initial Operating Capability
IS	Information System
IT	Information Technology
KO	Contracting Officer
LOA	Letter of Accreditation
LST	Local Standard Time
MS	Microsoft
MSSP	Microsoft SharePoint
NACI	National Agency Check with Inquiries
NARA	National Archives and Record Administration
NATO	North Atlantic Treaty Organization
NCIC-III	National Crime Information Center Interstate Identification Index
NDA	Nondisclosure Agreement
NIPR	Non-classified Internet Protocol Router
NIPRNet	Non-classified Internet Protocol Router Network
NLT	No Later Than
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
OGC	Office of the General Counsel
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
PDS	Permanent Duty Station

PDF	Portable Document Format
PII	Personally Identifiable Information
PHI	Personal Health Information
POC	Point of Contact
POI	Program of Instruction
PoP	Period of Performance
PRS	Performance Requirements Summary
PWS	Performance Work Statement
RM	Records Management
RMF	Risk Management Framework
RO	Responsible Officer
ROK	Republic of Korea
SA	Sponsoring Activity
SaaS	Software as a Service
SACO	Staff Action Control Officer
SCI	Sensitive Compartmented Information
SIPR	Secret Internet Protocol Router
SIPRNet	Secret Internet Protocol Router Network
SOFA	Status of Forces Agreement
SOP	Standard Operating Procedures
STIGs	Security Technical Implementation Guides
SWA	Southwest Asia
T&M	Time and Material
TAR	Travel Approval Request
TARP	Threat Awareness Reporting Program
TDY	Temporary Duty

TESA	Technical Expert Status Accreditation
TIM	Technical Interchange Meeting
TMT	Task Management Tool
TR	Technical Representative
TSDB	Terrorist Screening Database
USFK	U.S. Forces Korea
USG	United States Government