

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. CONTRACT ID CODE	PAGE OF PAGES
			J	1 35
2. AMENDMENT/MODIFICATION NO. 02	3. EFFECTIVE DATE 06-Mar-2015	4. REQUISITION/PURCHASE REQ. NO. SEESCHEDULE	5. PROJECT NO. (If applicable)	
6. ISSUED BY INSTAL & VEHICLE SUP CONTRACTING DIV 6501 E. 11 MILE ROAD WARREN MI 48397-5000	CODE W56HZV	7. ADMINISTERED BY (If other than item 6) INSTAL & VEHICLE SUP CONTRACTING DIV MELISSA BAYS CCTA-HDC-A/MS350 MELISSA.C.BAYS.CIV@MAIL.MIL WARREN MI 48397-5000		CODE W56HZV
8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code) UNIFIED BUSINESS TECHNOLOGIES, INC. MICHELLE D'SOUZA 353 INDUSCO COURT SUITE C TROY MI 48083-4646			9A. AMENDMENT OF SOLICITATION NO.	
			9B. DATED (SEE ITEM 11)	
			X	10A. MOD. OF CONTRACT/ORDER NO. W56HZV-11-D-L555-T032
			X	10B. DATED (SEE ITEM 13) 24-Sep-2014
CODE 3XMH1	FACILITY CODE 3XMH1			
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS				
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer <input type="checkbox"/> is extended, <input type="checkbox"/> is not extended. Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.				
12. ACCOUNTING AND APPROPRIATION DATA (If required) See Schedule				
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACT ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.				
A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.				
B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).				
X C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43.103(a)				
D. OTHER (Specify type of modification and authority)				
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copies to the issuing office.				
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) Modification Control Number: baysm15278 The purpose of modification 02 is to add funds for an existing labor category and fund an additional labor category. 1. SUBCLIN4000AH is established and funded for Program Manager hours. 2. SUBCLIN4000AJ is established and funded for System Engineer hours. 3. The total contract value is increased by \$ from \$, to \$2,708,358.38. 4. All other terms and conditions, except those addressed in the modification, remain unchanged and in full force and effect.				
Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.				
15A. NAME AND TITLE OF SIGNER (Type or print)			16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
			LYNNM.BYRNE/CONTRACTING OFFICER TEL: 586-282-6532 EMAIL: lynn.m.byrne.civ@mail.mil	

EXCEPTION TO SF 30
APPROVED BY OIRM 11-84

30-105-04

STANDARD FORM 30 (Rev. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY <u>Raymond M. Byrne</u> (Signature of Contracting Officer)	16C. DATE SIGNED 06-Mar-2015
---	------------------	---	-------------------------------------

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION A - SOLICITATION/CONTRACT FORM

The total cost of this contract was increased by \$167,153.60 from \$2,541,204.78 to \$2,708,358.38.

SECTION B - SUPPLIES OR SERVICES AND PRICES

SUBCLIN 4000AH is added as follows:

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4000AH	Year 4 - FFP-LOE	1	Job	\$	\$
	Non-Personal Services: Task Orders shall be issued against this CLIN using the labor rates established in Attachment 1 for year 1.				
	FOB: Destination				
	PURCHASE REQUEST NUMBER: 0010660091				
				NET AMT	\$
				CEILING PRICE	\$0.00
	ACRN AH				\$
	CIN: GFEB001066009100010				

SUBCLIN 4000AJ is added as follows:

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4000AJ	Year 4 - FFP-LOE	1	Job	\$	\$
	Non-Personal Services: Task Orders shall be issued against this CLIN using the labor rates established in Attachment 1 for year 1.				
	FOB: Destination				
	PURCHASE REQUEST NUMBER: 0010657838				
				NET AMT	\$
				CEILING PRICE	\$0.00
	ACRN AJ				\$
	CIN: GFEB001065783800001				

The following have been added by full text:

PERFORMANCE WORK STATEMENT

TACOMLCMC CIO/G6 Application Architecture Sustainment/Cyber Security/Information Technology Administrative and Management Support

A.Purpose:

1. To add IT labor hours and dollars to the contract for Application Architecture and database sustainment, technology insertion, technical study, capacity planning and performance management of the existing TACOMLCMC IT enterprise in support of TACOMLCMC/AMC Enterprise Architecture and Secure File Transfer (SFT) initiatives.

2. The Cyber Security Team has a requirement to provide TACOMLCMC customers and partners with the support needed to implement their Cyber Security requirements thereby enabling execution of the TACOMLCMC mission despite dynamic and changing DoD and DA level guidance. This support includes DoD Cyber Security Risk Management Model (Currently DIACAP which is in the process of transitioning to the Risk Management Framework (RMF) for DoD Information Technology (IT)), the Certificate of Networthiness (CoN) process, and Cyber Security administrative and operational governance services in support of DoD and Army Cyber Security regulations.

3. The Contractor shall utilize appropriate personnel with qualifications and experience encompassing the full range of IT; including knowledge of networks, communication, media services, desktop/laptop hardware and software configurations. The contractor shall have the IT skills to:

a. The Contractor shall have the ability to interpret technical and business work processes and determine if technical change or process change is required, IAW Basic Contract paragraphs C.5.6.

b. The contractor shall have excellent communication skills to include: research, writing, briefings, meetings and feedback. The contractor shall have technical knowledge of network operations, active directory, email and network communications; IAW Basic Contract BASIC PWS paragraphs C.5.1.

4. Support and maintain the DoD and DA Cyber Security policy, mandates, and procedures for implementing the Army Cyber Security Program, consistent with today's technological advancements for achieving acceptable levels of security in engineering, implementation, operation, and maintenance for information systems that are owned, managed, or operated by TACOMLCMC and Partners.

B.Skill Sets and Labor Hours: Hours and dollars on contract:

Total: \$2,708,358.38

C.CORs and COTRs: Government CORs and COTRs for each task order (TO) and project have been assigned by Appointment Letters from the Contracting Officer.

D.Description of Task Requirements:

Task 1.0. Web Design & Technical Writing: The objective of this task is to provide technical writing and web page design support to the CIO. The Contractor shall provide a qualified person for the task of senior web design and technical writing, IAW paragraphs C.5.4.3, C.5.4.12 and C.5.7 of the base contract PWS. The contractor shall perform senior web design and technical writing services for the CIO G6 office; these requirements can include documents that are routed to the CIO G6 from the Command Group and other G-Staff offices.

1.1. A summary of work completed shall be reported in CDRL A001, Monthly Status Report. The Contractor may use their own format or modify the DOD format for the Monthly Status Report, with the COTR's approval. The first reports shall be due forty-five (45) calendar days after contract award, with subsequent reports due every 30 days thereafter.

1.2. Contractor shall conduct editorial reviews to include review, revision and modification of document style layout, grammar and formatting for the following TACOM LCMC documents submitted for review IAW PWS Base C.5.2.12, C.5.4.2.c. and C.5.4.13. All documents that are provided by the Government shall be reviewed and updated by the suspense date assigned to each document; the task order COTR or designated Government

personnel will provide the contractor with the suspense dates.

- IM&T Business Plan
- IM&T Strategic Plan
- CIO/G-6 Action Plan for Command Staff Goals & Objectives
- CIO/G-6 Business Plan
- CIO/G-6 10-1
- CIO/G-6 Communications Plan
- CIO/G-6 Marketing Plan
- DIACAP documentation Templates
- Quarterly CIO/G-6 Newsletter
- Project Business Requirements Documents
- Project Technical Requirements Documents
- IT LCM Process Templates
- Business Requirements Document
- Technical Requirements Document
- Preliminary Proposal
- SIGACTs
- Staff Call Bullets
- BUA (Battle Update Assessments)
- Command Staff Documents
- System User Guides

1.3. The contractor shall review existing web pages on the TACOM LCMC Portal The contractor shall correct TACOM LCMC documents for 508 compliance issues, Personally Identifiable Information, integration and compatibility to the Portal SharePoint Software.

1.3.1. The contractor shall review, advise, and maintain content of the documents on the internet/intranet pages for the LCMC Portal and TACOM LCMC and Partners in accordance with organizational pages.

1.3.2. Contractor shall perform a review for Section 508 compliancy, by using Acrobat Professional software, for all newly developed web pages and documents as applicable. The contractor shall perform 508 compliancy fixes to TACOM LCMC organization web page content. All findings and recommendations shall be reported in CDRL A001, Monthly Status Report, due forty-five (45) calendar days after contract award, with subsequent reports due every 30 days thereafter.

1.3.3. Government will provide Government approved 508 software to all contractors who perform Portal web page development or sustainment.

TASK 2.0 Project Management: The contractor shall provide services in accordance with paragraphs C.5.7.1 of the Base Contract PWS as detailed below.

2.1. The contractor shall perform project requirements analysis, evaluation, planning,

design, management and documentation for CIO/G6, PEO GCS, ILSC & TARDEC task orders on contract W56HZV- 11-D- L555 and contract W56HZV-13-P-A751, in accordance with Best Business Practices, TACOMLCMC CIO/G6 Information Technology Life Cycle Management (ITLCM) and CDRL A007 Software Requirement Spec, under the authority of DID DI-IPSC-81439. The ITLCM process and document templates shall be provided by the Government within 45 days of contract award.

2.2. The contractor shall provide project management services as described below by applying industry best business practices in project management in conjunction with the TACOMITLCM methodology. The contractor shall execute required IT application support services within the specified cost, schedule and performance parameters of the individual task orders. The contractor shall perform the following in accordance with CDRL A005, Project Planning Chart due according to specific task order project plans:

- a. Project Planning using MS Project (Current version, (N+1, N-1))
- b. Project Scheduling, Task break down, Project Maintenance and Sustainment
- c. Project Cost Estimating, Cost and Resource Management
- d. Project Change Control
- e. Project Issue Assessment and Issue Tracking
- f. Project Risk Assessment, Risk Management and Risk Tracking

2.3. The contractor Project Manager (PM) shall initiate contact with CIO/G6, PEO GCS, ILSC and TARDEC task order COTRs to schedule individual project kick off meetings, to develop a project plan, project schedule and estimated cost for period of performance (POP) for each applicable project on the task order pursuant to details of the project kickoff meetings.

2.4. The contractor PM shall develop a project plan for CIO/G6, PEO GCS, ILSC and TARDEC task orders under the base contract if applicable. Baseline project plans shall be in accordance with CDRL A005, under the authority of DIDS DI- MGMT-80507A. The first project planning chart shall be provided to the COTR within forty-five (45) days after contract award. The baseline project plan shall be updated monthly and provided to the task order COTR by the last day of each month. The baseline project plan shall include contract tasks, schedule, cost, personnel issues, Government Furnished Property (GFP), and problems/issues for each project. Project planning should be done using MS Project (Current version, (N+1, N-1)). Any findings, results or actions accomplished during the previous 30 day reporting period shall be included in the Monthly Status report, IAW CDRL A001, and briefed at the subsequent project meeting. The contractor may use their own format or modify the DOD format, with the COTR's approval.

2.5. The contractor PM shall provide a monthly status report and PMR for CIO/G6, PEO GCS, ILSC and TARDEC task orders, IAW CDRL A001. The contractor may use their own format or modify the DOD format, with the COTR's approval. The monthly status report shall provide detail for all projects and tasks contained within each task order. The monthly status report shall contain at a minimum a task order breakdown to include tasks

completed, accomplishments, future objectives, risks/issues, contractor names and vacant positions.

2.6. All programs, systems planning, project planning, design, build and implementation shall adhere to the TACOM LCMC Enterprise Architecture main document to include annex A - C. The standard architecture will be provided to the contractor by the Government within 15 days of contract award.

Task 3.0 – 9.0 Summary of Task Order Effort: The Contractor shall be responsible for providing qualified personnel, to perform the following activities for the U.S. Army TACOM LCMC mission application architecture owned by CIO/G6: installation, configuration, integration, testing, troubleshooting, deployment, and sustainment of mission applications and/or systems, as defined in sections C.1.4.16, C.5.1, C.5.2, C.5.3, C.5.4, C.5.5, and C.5.6 of the basic PWS. The application architecture's services may span across multiple hosting sites where these work activities are to be performed including; Warren, APCs, DISA, and AMC selected sites or other commercial or remote sites. The Government will provide the technical requirements for the APC, DISA and AMC selected sites or other commercial or remote sites prior to contractor support in those areas. As needed, the Contractor shall be leveraged to support these activities not only with TACOM LCMC, but with other commands listed in Appendix A of the basic PWS to support U.S. Army enterprise activities. All processes, procedures, and documents created or modified shall be in accordance with (IAW) the following commercial standards: IT Infrastructure Library (ITIL) v3, International Organization for Standardization (ISO), and other industry best business practices <http://www.itil-officialsite.com/home/home.asp>.

Task 3.0 Government Incident, Problem, Change, Release, and Configuration Management: The contractor shall enhance and monitor the Government Incident, Problem, Change, Release, Configuration Management processes. The contractor shall verify software baseline configurations in coordination with the system owners and subsequent changes are stored in the Government software library system (when deployed) as well as any corresponding administrative information in accordance with the Contract PWS paragraph C.5.5.3. The system owner will inform the contractor of documented changes for their applications/systems. The Contractor shall report all software or configuration changes and administrative notations in the Monthly Contract Progress, Status and Management Report, IAW CDRL A001 for each subtask within Task 3.0. The first reports shall be due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format or modify DOD's format, with the COTR's approval.

3.1 The Contractor shall follow the established Government Incident, Problem, Change, Release, Configuration Management processes and procedures to enter descriptive information on all changes to enable tracking of approved hardware and software configuration and architecture changes for the production network in accordance with the Contract PWS paragraphs: C.5.4.13, C.5.4.5 and C.5.5. The COTR will provide the specific tracking elements of approved changes, to the contractor, within 120 days of contract award.

3.2 The Contractor shall monitor the performance of the Incident, Problem, Change, Release and Configuration Management processes and evaluate the effectiveness and efficiency of the processes and procedures and recommend process improvement and cost savings for the Government, as specified in paragraph C.5.4.5 of the Basic Contract PWS.

3.3 The Contractor shall adhere to DA/DoD regulatory guidance in support of DIACAP, security, and 508 Compliance as defined in the basic PWS sections C.1.3, C.5.2.12, C.5.4.13 and C.5.4.14.

3.4 The Contractor shall execute DIACAP efforts in accordance with DoD 8500.1, DoDI 8500.2, DoDI 8580.1, the acquisition life cycle requirements of DoDD 5000.1 and DoDI 5000.2, FISMA security requirements, Appendix III of OMB A-130, industry best practices, and lessons learned and as defined in the basic PWS C.5.2.12 and C.5.4.14. The Contractor shall make written recommendations to the COTR to reduce or eliminate any Information Assurance (IA) and security vulnerabilities or risks within the Application Architecture or mission application/systems. The Contractor shall create and update Standard Operating Procedures (SOP)s and desk procedures for all normal and emergency operations within the Application Architecture's mission area. The Government COTR will provide an initial SOP list within 120 days of contract award to be reviewed and modified quarterly. All SOP documents shall be provided to the COTR within 30 days of contract end date, IAW with basic Contract Appendix C, ITLCM process, and shall be written in accordance with CDRL A002, Technical Reports-Study, under the authority of DID DI-MISC- 808 0508A. The Contractor may use his own format or modify the DOD format, with the COTR's approval. All documents shall be electronically stored in an approved CIO/G6 Software/Document Library Tool and shall be version controlled as defined in the Basic Contract PWS C.5.4.6. The COTR will provide written procedure and access to G6 Repository for document storage to the contractor, within 60 days of contract award.

3.5 The Contractor shall document and record the Application Architecture, dependent technologies, and all hosted applications and/or databases starting from the initial baseline build or existing state, all subsequent configuration changes from the Government provided baseline IAW Basic Contract PWS C.5.5.2. The COTR will provide the information for the Baseline build for each server, application/system, database, storage and interfaces, within 30 days of contract award. All documents shall be provided to the COTR within 30 days of contract end date, IAW with basic Contract Appendix C and CDRL A002, Technical Reports-Study, under the authority of DID DI-MISC-8080508A.

3.6 The Contractor shall document and report to the COTR, any manual intervention taken to fix a problem/failure, within the Application Architecture. Manual interventions shall be reported to the COTR, by email, IAW with the contract PWS C.5.3 and IAW CDRL A002, Technical Reports-Study, under the authority of DID DI-MISC-8080508A. The Contractor may use his own format or modify the DOD format, with the COTR's approval. If the Contractor's manual intervention i s

taken to alleviate a software/hardware problem, a root cause analysis (Ishikawa Diagram) shall be completed and documented along with the corrective actions taken. The Contractor shall provide recommendations to prevent the same or similar problem/failure in the future. The COTR will provide the Root Cause Analysis Reporting template to the contractor within 120 days of contract award. The Root Cause Analysis and Contractor's recommendations shall be included in the Technical report in this paragraph IAW CDRL A002, due within 30 days of contract end date.

3.7 Contractors shall monitor log files and review scans to identify corrective actions, and work with the Government designated system IAM as needed IAW the basic PWS C.5.3.

Task 4.0 DATABASE MANAGEMENT (Oracle 10g, and 11g; Microsoft SQL 2008 and SQL 2012 Server):

The contractor shall provide the following database maintenance and sustainment services IAW Basic Contract PWS C.5.3. All maintenance actions shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001. The first reports shall be due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format or modify DOD's format, with the COTR's approval. The contractor shall:

- a. Install, configure and upgrade Oracle/SQL server software and related products
- b. Evaluate Oracle/SQL features and Oracle/SQL related products against industry standards
- c. Recommend sound backup and recovery policies and procedures.
- d. Monitor database security and create and maintain users and roles, assign
- e. Perform database tuning and performance monitoring
- f. Perform application tuning and performance monitoring
- g. Plan growth and changes (consider with capacity management requirements)
- h. Perform general technical trouble shooting and give consultation to development teams
- i. Interface with Oracle/Microsoft Corporation for technical support issues
- j. Patch Management and Version Control
- k. Apply Security Technical Implementation Guide (STIG) & Information Assurance Vulnerability Alert (IVA)
 - l. Mitigate vulnerabilities and create Plan of Actions & Milestones (POA&M's) on non-closed risks
 - m. Work with SA's to address settings and tuning system parameters.
 - n. Review data storage for the Database Management System (DBMS). Enable the DBMS to work with storage devices and storage management software.
 - o. Install COTS third-party DBA tools
 - p. Create and maintain Standard Operating Procedures (SOPs) to those items also defined in the database specific service catalog.
 - q. Work with System Owners to test Oracle 11g and SQL 2008 & SQL 2012.

4.1 The Contractor shall perform the following systems administration services as defined in the Basic Contract PWS C.5.3:

- a. Add New Accounts by assigning Application ID's and User ID's
- b. Create the APPUSER profile and set the Expiration to 365 Days
- c. Create DB_USERS profile and set the Expiration according to current DoD and Army Information Assurance requirements
- d. Provide guidance to end users for resetting expired Passwords

4.2 The Contractor shall perform the following Daily Tasks as defined in the Basic Contract PWS C.5.2 through C.5.2.18:

- a. Check Database Backups and Archive log weekly to ensure completeness, frequency and accuracy
- b. Space Utilization on Servers
- c. Check for Outstanding Alerts, Invalid Logins to database
- d. Check Monitoring Table to Ensure Scheduled Jobs ran successfully
- e. Monitor databases throughout the day to identify any potential issues such as database locks, bottlenecks, and hack attempts.
- f. Utilize NEC Commvault POC for backup services for file and database backups.

4.3 The Contractor shall perform the following Weekly Tasks as defined in the Basic Contract PWS C.5.3.13:

- a. Review Expired IDs. (Automated script to list expired and about to be expired IDs)
- b. Send Reminder EMAIL to ID owners who are going to expire
- c. Monitor log files monthly and document all problem areas/issues

4.4 The Contractor shall perform the following Monthly /Quarterly Tasks as defined in the Basic Contract PWS C.5.2 and C.5.2.4:

a. Send Monthly Audit Report to designated COTR and designated system IAM. Reports shall be in accordance with CDRL A002, Technical Reports Study, under the authority of DID DI- MISC-8080508A. Reports due the first business week per Month after contract award date. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

b. Update metrics on DBMS performance and availability. The Contractor shall review results with the COTR by the first business day of each week after contract award date. The Contractor shall use the standard reporting capabilities of Oracle and SQL.

c. Implement Quarterly Patches. This is a several week process as Development is targeted first and tested before Production Implementation. Contractor shall provide quarterly reports showing that quarterly patches have been applied to all working environments and indicate the version of the applied patch. Reports shall be in accordance with CDRL A002, Technical Reports Study, under the authority of DID DI- MISC-8080508A. Reports are due by the second business week per Quarter after

contract award date. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

d. Test Database Restore and Restore File recovery on a quarterly basis to ensure databases are recoverable. Following the CIO/G6 Backup & Recovery/Business Sustainment document, the Contractor shall provide a report showing successfully tested restores of randomly chosen databases selected by the COTR. Reports shall be in accordance with CDRL A002, Technical Reports Study, under the authority of DID DI-MISC-8080508A. The first reports shall be due the first business week per Quarter after contract award. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

4.5 Information Assurance Services: The Contractor shall provide Information Assurance support IAW Basic Contract PWS C.5.2.8. All results for tasks 3.5.1 through 3.5.2 of this task order shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001. The first reports shall be due by due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format or modify DOD's format, with the COTR's approval.

4.5.1 The Contractor shall configure DBMS to be IAW AR 25-2 & sufficient Password Complexity Requirements.

4.5.2 The contractor shall evaluate vulnerability report for identification and elimination of security vulnerabilities.

4.6 The Contractor shall provide Sustainment and Production Support for databases/ instances over the life of the contract as defined in the Basic Contract PWS C.5.3. The Contractor shall perform the following System Database administration tasks as well as those defined in the database specific service catalog:

a. Maintain the database servers and services so that they are up and functioning during normal business hours as stated in Basic Contract PWS C.1.9.1. Provide recommendations to System Owners on application administration responsibilities as defined in the Basic Contract PWS C.5.3.

b. Investigate questions from System owners and/or users regarding functions of the application that are not working as expected. Correct configurations or settings where appropriate.

c. Apply required security and vendor supplied patches and updates to the database application software. Test and verify all required patches and updates to determine if they are successful IAW C.5.2.4 of the Basic Contract PWS. The Contractor shall update baseline documents impacted by the changes. All document updates shall be in accordance with CDRL A015, Software documentation, under the authority of DIDS: DI- IPSC- 81756, due 30 days after receipt of the patch from the vendor NEC. The Contractor may use his

own format or modify the DOD format, with the COTR's approval.

d. Provide recommendations to System Owners to enable them to complete the DIACAP process for their databases/instances related to application /system as defined in the Basic Contract PWS C.5.8.

e. The Contractor shall schedule backups of mission databases to act as the first line of defense to be able to restore databases to normal operations.

TASK 5.0 APPLICATION ARCHITECTURE SUSTAINMENT, TECHNOLOGY INSERTION and Secure File Transfer Protocol (sFTP): The Contractor shall provide technical knowledge, expertise and resources to sustain TACOM LCMC centralized mission application/systems or executive/enterprise software products hosted within the Application Architecture boundaries for TACOM LCMC and its functional or partner commands.

5.1 The Contractor shall make recommendations to improve existing or develop processes that impact workflow to improve speed of delivery and/or quality of services IAW Basic Contract PWS C.5.4.2. The Contractor shall work with the Government to research other ITIL Service Operation processes as to document and incorporate links into the following sub- processes: Event, Incident, Request, Problem, and Configuration management processes. All actions shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001. The first reports shall be due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format or modify DOD's format, with the COTR's approval.

5.2 The Contractor shall provide LifeCycle Management as a function responsible for managing MPC-AAS applications/software versions. This includes the documenting, testing, and recommendation on improvement of applications/software offered by the MPC-AAS.

5.3 The Contractor shall support the IT Service Management Lifecycle to transition, operate and make recommendations to improve -MPC-AAS service offerings. Once the Government implements a centralized software library, the Contractor shall only deploy applications/systems or changes from this repository as the approved source to be used in the pre- production and production environments. All actions shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001. The first reports shall be due the first business week of each month.

5.4 The Contractor shall:

a. Monitor application servers and services to ensure they are up and functioning and shall monitor application/systems for availability and performance IAW Basic Contract PWS C.5.13.1.2.

b. Interface directly with all stakeholders as needed, including the System Owners, Users, CIO/G6 or AMC groups. The Contractor shall resolve any access issues that

users may be having in relation to any applications within their control. These may range from desktop configuration issues or client software issues IAW Basic Contract PWS C.5.3.2, C.5.3.3, and C.5.4.

c. Respond to individual users' difficulties with application/systems, provide instructions and training, and diagnose and solve common problems. These may be desktop configuration issues or client software issues IAW Basic Contract PWS C.5.3.2, C.5.3.3, C.5.4, and C.5.4.18.

d. Investigate questions from users regarding functions of the application that are not working as expected. Correct configurations or settings to ensure application has correct configurations and settings IAW Basic Contract PWS C.5.3.1 and C.5.6.

e. Work with third-party software providers to resolve questions or problems with the operation of the software if local settings or configurations are not successful IAW Basic Contract PWS C.5.3.1 and C.5.4.17.

f. Work with CIO IA as directed by the COTR to assist, document, test, and verify all required patches and updates to the application software whether provider supplied or required by IAVA IAW Basic Contract PWS C.5.2.3 and C.5.2.4.

g. Support System Owners with their application/systems DIACAP requirements IAW Basic Contract PWS C.5.2.3.

h. Assist with CIO IA as directed by the COTR with possible errors and access violations to system and application logs IAW Basic Contract PWS C.5.3, C.5.3.1, C.5.3.3, C.5.3.4 and the Cyber Incident Response Policy dated 25 March 2013.

i. Work with System Owners to monitor the application and its operating environment(s) and ensure they are backed up at the proper intervals to meet documented Government COTR provided restore requirements. If the restore requirements do not exist, the Contractor shall work with the Government to document these requirements with the System and Business Process owners IAW Basic Contract PWS C.5.2.3.

j. On an annual basis and following the CIO/G6's Backup & Recovery/Business Sustainment document, the Contractor shall work with the System Owners and provide a report showing successfully tested restores for all support application/systems. The Government COTR will provide the list of applications on App Infrastructure along with systemowner names, phone numbers, email as well as proposed date of annual review for each of the applications within 90 days of contract award IAW Basic Contract PWS C.5.2.3.

k. Maintain user authentication, as well as AKO single sign-on authentication and whatever new authentication piece the Army releases when applicable, to the TACOM

LCMC Applications IAW Basic Contract PWS C.5.3. The COTR will coordinate NEC participation for assistance and access to Network infrastructure information. The COTR will provide the following: firewall policies, reverse proxy rules and policies, patch installs, network monitoring policies, client image PC rules and policies, back-up policies and procedures for each of the servers and environment within 120 days of contract award.

1. Migrate to newer hardware, virtualization or upgrade to supported versions as older versions expire. The migration to future Operating Systems requires testing to ensure that all supported applications are operable under the newest version of the operating systems as defined in the Basic Contract PWS C.5.3.1, C.5.3.2, and C.5.3.

5.5 The Contractor shall consult remotely with all TACOM LCMC sites and System Owners to deploy CIO/G6 approved transfer technologies at their local sites. The Contractor shall interface with other technical teams located across multiple commands in order to help establish the proper point-to-point communication channels between sites and/or applications. All findings and results are to be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001. Reports are due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format or modify DOD's format, with the COTR's approval.

5.6 The Contractor shall act as AMC's Logistical System Support Office (LSSO's) technical Subject Matter Expert to support all AMC sites and System Owners remotely to deploy selected AMC approved technologies. The Contractor shall support LSSO and AMC to analyze data call results in order to help itemize and prioritize the AMC's deployment efforts. The Contractor needs to be able to interface with other technical teams located in other commands in order to help establish the proper point-to-point communication channels between sites and/or applications. All findings and results are to be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001. Reports are due the first business week of each Month after contract award.

5.7 The Contractor shall test newer software versions and vendor security patches. The Contractor shall create the proper test cases and document the results for the Government to review. The Contractor shall follow the Government's change and release processes to deploy approved changes into its pre-production and production environments. The Contractor shall create all required paperwork to obtain TCoNs and/or CoNs as requested by the Government.

5.8 The Contractor shall follow the Government's approval process to provide applications or individuals access to the secure file transfer technologies located at the US Army Garrison - Detroit Arsenal, Warren, MI. The goal is to centralize and manage secure file transfer Capabilities.

5.9 The Contractor shall create and maintain "Managing Secure File Transfers – Jumpstart Plan" report to be used by any AMC site or System Owner on the activities needed to successfully deploy using AMC's secure file transfer technologies. The Contractor shall also create and maintain Standard Operating Procedures (SOPs). Within 30 days after contract

award, the Contractor shall review with the Government, all reporting types offered by the vendors COTS software. The Government will select which additional COTS reports are needed within 7 business days after the review.

5.10 The Contractor shall act as the Subject Matter Expert and shall attend meeting. These meetings include those scheduled by AMC, AMCLSSO, or TACOM as defined in the Basic Contract PWS C.1.17, C.1.17.2, and C.1.17.8.

5.11 The contractor shall create and maintain software build guides as directed by the COTR. The contractor shall use the latest build guide template provided by the local NEC to prepare assigned guides. Any contractor who installs software will adhere to the build guide directions and will not install any software, modules, add-ons, that are not documented.

TASK 6.0 TACOM LCMC PORTAL SUSTAINMENT: The Contractor shall provide technical knowledge, expertise and resources to sustain TACOM LCMC portal / TACOM LCMC Site Collections, to include supporting and maintaining portal third party tools / custom webparts.

6.1 Enterprise Content Integration: The contractor shall provide portal system integration and hardware/ software architecture support to maintain the TACOM LCMC Portal / TACOM LCMC Site Collections and its integrated application capabilities. The Contractor shall customize and extend the existing and future TACOM LCMC Portal / TACOM LCMC Site Collections and features as determined by the COTR. The Contractor shall maintain and support enterprise content integration within the LCMC portal to include content indexing, search configuration, server configuration, and access control IAW with the basic PWS C.5.4.3.

6.2 Portal Software Monitor Maintenance: The Contractor shall monitor access rights, security, SharePoint application, and user event log files on production, QA and development server environments IAW with the basic PWS C.5.3.10.2. The Government will provide access for contractor to perform task items within this task order.

6.3 The contractor shall Analyze/Troubleshoot/Implement/ the NEC IA patches and directives in accordance with Basic Contract paragraph C.5.4.11.1.

a. The Contractor shall monitor TACOM Network Enterprise Center (NEC) / LAN Services applied patches and updates on production, QA, and development server environments IAW the basic PWS C.5.3. and the Vulnerability Management plan v1.1. The Contractor shall perform troubleshooting and identify issues with applied patches on all server environments. All findings, recommendations and actions shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI- MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

b. The Contractor shall provide technical information as a participant in hardware and Commercial Off-the-Shelf (COTS) software Test Groups for the CIO/G6 and the IT Services Contract COTRs IAW the basic PWS C.5.4. COTS Software shall be tested to the Government's functional and technical specifications. The COTR will provide functional and technical specifications to the contractor prior to on-start of testing. All findings and test results and recommendations shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

c. The contractor shall troubleshoot, analyze and research hardware/software updates and changes. The Contractor shall perform an impact analysis to the existing applications and integrated applications, of these changes IAW the basic PWS C.5.4. The Contractor shall report all findings, research, results and recommendations in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

6.4 Production, QA, and Dev, Admin Support: The Contractor shall provide Production, QA and Development application administration (ADMIN) support in accordance with paragraphs C.5.2 of the Basic Contract PWS. The Contractor shall report all findings and recommendations in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

6.5 Portal Administrative Support: The Contractor shall perform services in accordance with paragraphs C.5.3 of the Basic Contract PWS and detailed in paragraph 5.5.1, 5.5.2 and 5.5.3 of this task order.

6.5.1 Monitor Maintain User profiles/security: The Contractor shall monitor user authentication to LCMC Portal. The Government will be responsible for providing the contractor access to NEC personnel for assistance and access to Network infrastructure information. The Government will provide the following: firewall policies, reverse proxy rules and policies, patch installs, network monitoring policies, client image PC rules and policies, back-up policies and procedures for each of the servers and environment. The Contractor shall report all actions in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

6.5.2 Portal Production Monitoring: The Contractor shall monitor

performance of the TACOM LCMC portal for availability, access, speed, security, application integration, performance and user event log files IAW of the basic PWS C.5.13.1.2. The Contractor shall report all findings, research, results and recommendations in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

6.5.3 Portal Maintenance: The Contractor shall provide portal maintenance scans to all Government and non Government farm/site collection administrators as described in the TACOM LCMC portal governance plan. The COTR will provide the governance plan to the contractor within 5 days of contract award.

6.5.4 All contractors with SharePoint elevated rights shall abide by the policies and procedures as described in the TACOM LCMC portal governance plan. The COTR will provide the governance plan to the contractor within 5 days of contract award.

6.5.5 The Contractor shall design and help create, sustain, and troubleshoot SharePoint 2010 (N+1, N-1) Workflows via GUI, InfoPath, SharePoint Designer 2010 (N+1, N-1), and Visual Studio 2010 (N+1, N-1), Kendo UI, TELRIK and Silverlight. The Contractor shall liaise with CIO G6 SharePoint administrators and help solve all user issues as they arise.

6.6 Information Assurance: The Contractor shall perform DIACAP Information Assurance Certification and Accreditation tasks to ensure internal controls are in place and functioning, in accordance with C.5.4.11 of the Basic Contract PWS. Government will perform inspections and sample testing of the system. All actions to strengthen or add internal controls shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

6.7 SharePoint Migration: The Contractor shall assist with the migration of the TACOM LCMC SharePoint Portal to the current version (N+1, N-1) of SharePoint. The contractor shall assist with the design, planning and project management of the migration of the SharePoint Portal to DISA / AMC or any other organization determined by the Government, IAW the BASIC Contract PWS, paragraphs C.5.7.1 and C.5.7.2. The contractor shall report all actions, findings and recommendations in accordance with CDRL A007 Software Requirement Spec, CDRL A008 Implementation Plan, CDRL A014 Software Development Plan, and/or CDRL A015, Software Documentation. The contractor shall report all actions, findings and recommendations in CDRL A001, Monthly Status Report and shall be included in the monthly updates to CDRL A005 Project Planning Chart. The Contractor may use his own format for the above CDRLS in this paragraph due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

Task 7.0 SHAREPOINT SUSTAINMENT

7.1 The Contractor shall supply a senior level SharePoint SME with architecting, implementing, sustaining, and troubleshooting high-end, highly available SharePoint web farms. The SharePoint SME shall have extensive experience in SharePoint Server (SPS) 2010 (N+1, N-1), along with Microsoft SQL Server 2005/8 (N+1, N-1). The contractor shall design leading edge SharePoint solutions and provide support for CIO G6 hardware and software platforms, such as SharePoint servers, .NET web servers, reporting tools, access, communications, performance monitoring and other associated capabilities. The contractor shall create an environment and culture for maintaining highly secure and available systems through the implementation of industry standard best practices along with designing, implementing and maintaining SharePoint and reporting services. The contractor shall provide direction for the management, design and performance tuning of CIO G6 hardware and software.

7.2 The Contractor shall review the existing IT infrastructure, business processes, application flows, interfaces, interoperability, and customer applications and then provide the direction needed to gain further efficiencies in robustness, customer satisfaction, scalability, and redundancy. All actions shall be reported under CDRL A001, Monthly Status Report, under the authority of DI-MGMT- 80227(T). Reports are due 45 days after contract award, then every 30 days thereafter. The Contractor may use his own format or modify the DoD format, with the COTR's approval.

7.3 The Contractor shall architect and modify the CIO G6 server farm to maximize performance in accordance with industry and manufacturer best business practices with regard to hardware and software. Configuration sustainment and changes shall be documented and submitted to the COTR request. The Contractor shall document Configuration sustainment, changes, findings, research, results and recommendations in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

7.4 The Contractor shall be the Subject Matter Expert for the complete CIO G6 SharePoint farm and TACOMLCMC Site Collections.

7.5 The Contractor shall design and direct the installation, sustainment, troubleshooting, and implementation of a SharePoint web application and associated database backup and disaster recovery plan: liaise with the CIO G-6 to determine and implement a best solution; perform disaster recovery tests on a scheduled basis; design disaster recovery plan and keep updated; and coordinate test backups to make sure that they work. All actions shall be reported under CDRL A001, Monthly Status Report, under

the authority of DI-MGMT-80227(T). Reports are due 45 days after contract award, then every 30 days thereafter. The Contractor may use their own format or modify the DoD format, with

the COTR's approval.

7.6 The Contractor shall install, sustain, upgrade, migrate and troubleshoot Microsoft Office SharePoint 2010 (N+1, N-1). The Contractor shall liaise with CIO G6 SharePoint administrators and help solve all user issues as they arise. The Contractor shall monitor, plan and configure SharePoint application services. The Contractor shall setup, monitor and tune server performance utilizing built-in performance counters. The Contractor shall be familiar with configuring and implementing different modes of authentication such as standard Windows authentication, Claims-based authentication and SAML Token-based authentication and Active Directory Federation Services (ADFS) 2.0. All actions shall be reported under CDRL A001, Monthly Status Report, under the authority of DI-MGMT-80227(T). Reports are due 45 days after contract award, then every 30 days thereafter. The Contractor may use his own format or modify the DoD format, with the COTR's approval.

7.7 The Contractor shall design and direct the installation, sustainment (patching), and troubleshooting of a Server farm supporting Microsoft Internet Information Services (IIS) 7 (N+1, N-1). The Contractor shall install .NET Framework 2.x, 3.x, and 4.x Microsoft C# web applications that are developed in-house or by external contractors. The Contractor shall work with the NEC and TNOSC when setting up URLs, FQDNs, IPs, and DNS and configuring the Firewall and Reverse Proxy with assistance from the COTR.

7.8 The Contractor shall design and direct the creation, sustainment, and troubleshooting of SharePoint's Business Data Services (BDS) for 2010 (N+1, N-1) with direction from the COTR.

7.9 The Contractor shall design and help create, sustain, and troubleshoot SharePoint 2010 (N+1, N-1) Workflows via GUI, InfoPath, SharePoint Designer 2010 (N+1, N-1), and Visual Studio 2010 (N+1, N-1), Kendo UI, TELRIK and Silverlight. The Contractor shall liaise with CIO G6 SharePoint administrators and help solve all user issues as they arise.

7.10 The Contractor shall architect, plan, communicate, and perform SharePoint migrations from 2010 to 2013 when determined by the Government. All actions shall be reported under CDRL A001, Monthly Status Report, under the authority of DI-MGMT-80227(T). Reports are due 45 days after contract award, then every 30 days thereafter. The Contractor may use his own format or modify the DoD format, with the COTR's approval.

TASK 8.0 TACOMLCMC SharePoint Portal

8.1 Enterprise Content Integration: The Government will provide all source code for web services and existing authentication documentation for each of the following: ColdFusion applications, portal account application and Security Roster. The contractor shall not perform any new change requests/enhancements as these are in sustainment mode. The Contractor shall maintain and support enterprise content integration within the LCMC portal to include personalization of portal pages and 508 compliancy with the basic PWS C.5.4.9

and PWS Appendix F.

8.1.1. The Contractor shall attend and actively participate in weekly meetings in support of the TACOM LCMC Portal and provide technical information supporting areas of analysis, testing, implementation and maintenance, IAW paragraphs C.5.3.9 of the basic contract PWS.

When feasible, the Contractor shall perform source code management, environment management and production code deployment utilizing COTS software provided by the Government. All contractor developed source code shall be in compliance with CDRL A010 Computer Software Product, Source Coding. All software shall be installed and tested on Government specified computer and operating system. The Government will provide the specifications for the format and content of all source code. The Government will supply all existing COTS products to the contractor within 30 days of contract award, IAW paragraph C.5.3.11 of the basic contract PWS.

8.1.2. The Contractor shall prepare and maintain test plans, documentation, and system management plans. The contractor shall submit documentation and plans IAW CDRL A004, Software Test Plan. All findings and recommendations shall be reported under CDRL A001, Monthly Status Report. The Contractor may use his own format or modify the DoD format, with the COTR's approval, IAW paragraphs C.5.3.11 of the basic contract PWS.

8.2 TACOM LCMC Organizational support: The contractor shall consult with the ILSC, command staff and other organizations' web master/poster personnel with web page and development and design issues. The Contractor shall analyze, troubleshoot and provide solutions to WEB Page issue IAW paragraphs C.5.4.9, C.5.3.3 of the basic contract PWS. All findings, recommendations and actions shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI- MGMT- 80227(T), due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

8.2.1 All contractors with SharePoint elevated rights shall abide by the policies and procedures as described in the TACOM LCMC/ AMC portal governance plan. The COTR will provide the governance plan to the contractor within 5 days of contract award.

8.2.2 The Contractor shall design templates, layouts, graphics, animations and other related materials in support of TACOM LCMC portal using web graphic design tools that have been designated as standard TACOM automated tools such as Designer, Infopath, Adobe Photoshop, Visual Studio 2010 (N+1)(N-1) and that are included in the TACOM LCMC IT Architecture. The contractor shall provide complete WEB Pages IAW CDRLS A010, Computer Software Product-Source Coding. The contractor shall install and test all Web Pages on Government specified computer and operating system. The Government will provide the specifications for the format and content of all source code. All findings and recommendations shall be included in CDRL A001, Monthly Status Report and shall be documented in CDRL A005, Project Planning Chart. The Contractor may use his own format

or modify the DoD format, with the COTR's approval, IAW paragraphs C.5.4.9 of the basic contract PWS.

8.2.3 The Contractor shall maintain currency of knowledge with respect to relevant, state-of-the-art application design and development methodologies and provide innovative solutions, IAW paragraphs C.5.4.9 of the basic contract PWS.

8.2.4 The Contractor shall develop and maintain test plans, documentation, and system management plans. The contractor shall submit documentation and plans IAW CDRL A004, Software Test Plan. All findings and recommendations shall be reported under CDRL A001, Monthly Status Report under authority of DID DI-MGMT-80227(T), due 45 days after contract award, then every 30 days thereafter. The Contractor may use his own format or modify the DoD format, with the COTR's approval, IAW paragraphs C.5.3.11 of the basic contract PWS.

8.2.5 When new projects are brought on board, the Government COTR will assign projects to the contractor and the Contractor shall provide meaningful evaluation and measures into the selection process of automated tools to support Project Management, Enterprise Architecture, TACOM LCMC Portal, Configuration Management, Data Warehousing, Enterprise Content Management (ECM) and Knowledge Management, through cost benefit analysis, product evaluation and requirements definition. The Contractor shall coordinate and participate in the implementation and integration of the above tools, as well as, establish and populate baselines within the tools. All contractor developed source code shall be in compliance with CDRL A010 Computer Software Product-Source Coding. The contractor shall install and test all software on Government specified computer and operating system. The Government will provide the specifications for the format and content of all source code. The Contractor may use his own format or modify the DoD format, with the COTR's approval, IAW paragraphs C.5.5.3 of the basic contract PWS. The contractor shall report all actions, findings and recommendations in CDRL A001, Monthly Status Report and shall be included in the monthly updates to CDRL A005 Project Planning Chart. The Contractor may use his own format for the above CDRLs in this paragraph due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

8.2.6 The Contractor shall design and help create, sustain, and troubleshoot SharePoint 2010 (N+1, N-1) Workflows via GUI, InfoPath, SharePoint Designer 2010 (N+1, N-1), and Visual Studio 2010 (N+1, N-1). The Contractor shall liaise with CIO G6 SharePoint administrators and help solve all user issues as they arise.

8.3 Portal Training: The Software Architect contractor shall provide one-on-one or group training, IAW the Basic Contract PWS, paragraphs C.5.4.16, C.5.4.16.1. Training will consist of up to 30 people per month, for not longer than 4 hours each. The contractor shall provide guidance to Government Web Masters and portal users, in SharePoint software and TACOM LCMC Portal use. All actions shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001, under authority of DID DI-MGMT-80227(T),

due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

8.4 SharePoint Migration: The Contractor shall assist with the migration of the TACOM LCMC SharePoint Portal to the current version (N+1, N-1) of SharePoint. The contractor shall assist with the design, planning and project management of the migration of the SharePoint portal to DISA / AMC or any other organization determined by the Government, IAW the BASIC Contract PWS, paragraphs C.7.1 and C.5.7.2. The contractor shall report all actions, findings and recommendations in accordance with CDRL A007 Software Requirement Spec, CDRL A008 Implementation Plan, CDRL A014 Software Development Plan, and/or CDRL A015, Software Documentation. The contractor shall report all actions, findings and recommendations in CDRL A001, Monthly Status Report and shall be included in the monthly updates to CDRL A005 Project Planning Chart. The Contractor may use his own format for the above CDRLS in this paragraph due 45 days after contract award, then every 30 days thereafter. Contractor may use his own format for this report, or modify DOD's format, with the COTR's approval.

TASK 9.0 TACOM LCMC Application Support

9.1 The Contractor shall provide support for systems, applications, web pages, scripts, and technical/functional documents that support the TACOM LCMC CIO G6 mission IAW Basic contract PWS C.5.15.1 and C.5.4. This support shall include design, development, updates, review, technical advising, collaboration, migration, modernization, maintenance, sustainment, testing, technical writing, briefings, manuals, user training, documentation, meeting attendance, and the implementation of information assurance controls. System/application environments include, but are not limited to, Visual Studio, ColdFusion, .NET, SharePoint, HTML, JavaScript, SQL Server, etc.

9.2 All development pages shall be in compliance with section 508 standards.

9.3 All findings shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001. The first Report shall be due forty-five (45) calendar days after contract award, with subsequent Reports due every 30 days thereafter.

9.4 All documentation shall comply with CDRL A015, Software Documentation, under the authority of DID DI-IPSC-81756, due 30 days before contract end-date. The Contractor may use his own format for the Monthly Contract Progress report or modify the DOD format, with the COTR's approval.

Task 10.0 DIACAP/RMF for DoD IT IMPLEMENTATION AND SUPPORT: The contractor shall disseminate and support the CIO/G6 Risk Management business processes, within TACOM LCMC and Partners, IAW Section C.5.8 of the Basic Contract PWS. The contractor shall develop guidance, procedures and training for System Owners and organizations, who have previously implemented DIACAP or in the process of transition to the RMF for DoD IT process IAW C.5.2.11, C.5.4.16. All training shall be in

compliance with Section 4.5 of this task order. All completed actions and status for this tasks and sub-tasks shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001, due 45 days after contract award, then every 30 days thereafter. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

10.1 The contractor shall perform working group sessions with system owners to discuss current status, analyze the issue from a Cyber Security perspective, and work with the system owner to help determine possible resolution of any issues for recommendation to Government on applications, information systems, AIS or systems as documented within DoD 8500 series, NIST 800 special publications, and the Committee on National Security Systems Cyber Security issuances. Working group sessions will be performed based on IT lifecycle schedule requirements that range from weekly to quarterly dependent on lifecycle phase with contractor and Government analysis of system owner requirements. The contractor is responsible for working with the system owner to schedule and develop agenda. Actions and minutes resulting from the working group will be recorded within C&A team collaborating tools and the contractor shall track resulting actions items IAW the Basic Contract PWS paragraphs C.5.8., C.5.8.1, C.5.8.2 and C.5.6.7. All completed actions and status shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001, due 45 days after contract award, then every 30 days thereafter. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

10.2 The contractor shall provide one-on-one customer support, consulting, training and oversight, IAW the Basic Contract PWS, paragraphs 1.4.8.1.1, through the DIACAP/RMF for DoD IT processes. All training shall be in compliance with section 4.5 of this task order. The contractor shall be responsible for advising System Owners with recommendations to the standard TACOM LCMC processes and Templates, administering and guiding System Owners through the process to include a review of completed accreditation documentation to verify that it meets DoD and DA standards. The contractor shall document all compliance issues and recommendations IAW the Contractor's Monthly Contract Progress, Status and Management Report, CDRL A001, under the authority of DID DI- MGMT- 80227(T), due 45 days after contract award, then updates are due every 30 days thereafter. The Contractor may use his own format or modify the DOD format, with the COTR's approval. The Government COTR will provide contractor with the TACOM LCMC Templates within 15 days of contract award and instruction for verification of meeting COTR defined standards within 30 days of contract award.

10.3 The Contractor shall identify any known TACOM LCMC and Partners' owned, sponsored or developed unique applications, information systems, AIS and systems that are not in compliance with the standards and regulations stated in Appendix F of the basic contract and Section E, paragraph 4 of this task order. The contractor shall research and analyze based on applicable standards, regulations, processes and the application of the contractors knowledge to the current DoD GIG operating environment to develop a course of action for each assigned application, IS, AIS or system to meet compliance

requirements. The Contractor shall recommend the course of action to the Government based upon knowledge of standards, regulations and processes in Appendix F of the basic contract and Section E, paragraph 4 of this task order and application of the contractor's knowledge of the current DoD Global Information Grid (GIG) Certification & Accreditation (C&A) environment. The Government will review the contractor provided recommendation and will make an internal course of action decision IAW contract Basic Contract PWS C.5.8, C.5.8.1, and C.5.8.2 with no impact to the contractor's performance. The contractor shall document all compliance issues and recommendations IAW the Contractor's Monthly Contract Progress, Status and Management Report, CDRL A001, under the authority of DID DI-MGMT-80227(T), due 45 days after contract award, then updates are due every 30 days thereafter. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

10.4 The contractor shall monitor and track the System Owners' progress towards the Authority to Operate (ATO) decision within the DIACAP/RMF for DoD IT Processes, using the Government provided C&A Repository, the Army Portfolio Management Solution (APMS), the SIPRNet Global Information Grid Interconnection Approval Process System (SGS), Defense Switched Network (DSN), Applicable Fiscal Year (FY) Federal Information Security Management Act (FISMA) reporting, the Army C&A Tracking Database, Enterprise Mission Assurance Support Service (eMASS), and the Systems/Networks Approval Process (SNAP) IAW the contract Basic Contract PWS C.5.7.1. The contractor shall provide email notification alerts to the System Owner and the TACOM Cyber Security Team when system authorization documentation must be updated or expires in the weekly team administration meetings. The Government will provide tools and information required to obtain access to the various progress reporting tools to the Contractor within 15 days of contract award. The contractor shall require read access to all tools to track C&A progress; write access shall be granted to the contractor for the C&A Repository and Army C&A Tracking Database to execute updates as required. The contractor shall document all compliance issues and recommendations IAW the Contractor's Monthly Contract Progress, Status and Management Report, CDRL A001, under the authority of DID DI-MGMT-80227(T), due 45 days after contract award, then updates are due every 30 days thereafter. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

10.5 The contractor shall coordinate quarterly POAM reviews with the system owners of their assigned IT systems and ICANs to ensure the assigned systems meet the requirements as outlined within the regulations identified within Appendix F of the basic contract and Section E, paragraph 4 of this task order as defined in the Basic Contract PWS C.5.4.2, C.5.2.9, C.5.2.10, C.5.8.2. The Government will provide the assigned IT systems within 15 days of contract award and will update quarterly as required. The contractor shall document any gaps between the systems' system authorization documentation / artifacts and the regulations in Appendix F of the basic contract and Section E, paragraph 4 of this task order discovered as a result of this review and provide recommendations for compliancy using knowledge of standards, regulations and processes in Appendix F of the basic contract and Section E, paragraph

4 of this task order application of the contractors knowledge to the current DoD Global Information Grid (GIG) Certification & Accreditation (C&A) environment to the Government IAW the Contractor's Monthly Report, CDRL A001, under the authority of DID DI- MGMT-80227(T), due every 30 days. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

10.6 The contractor shall perform a yearly evaluation of each assigned system, as required by the system, application, or information system lifecycle in the form of a contingency plan test, IA annual control review test and an IA annual review per the standards and regulations stated within Appendix F of the basic contract and Section E, paragraph 4 of this task order and any TACOM LCMC specific processes which will be provided within 30 days of contract award as defined in the Basic Contract PWS C.5.4.13 and C.5.8.2. The contractor shall contact the System Owner through email to begin yearly evaluation NLT three months prior to expiration and will provide documentation completed by the System Owner along with recommendation made using knowledge of standards, regulations and processes in Section F and Section E, paragraph 4 of this task order application of the contractors knowledge to the current DoD Global Information Grid (GIG) Certification & Accreditation (C&A) environment to the Government NLT than three weeks prior to expiration. Any issues in obtaining System Owner completed documentation should be reported to the Government COTR no later than 5 weeks prior to expiration.

Task 11.0 CoN IMPLEMENTATION AND SUPPORT: The contractor shall work with TACOM LCMC customers and partners towards the completion of Application and System Certificate of Networthiness (CoN) to include processes required by TACOM LCMC and the IT service provider and the review of System, Application and Test CoN checklists to verify that they meet process standards as defined in the Basic Contract PWS C.5.4.13 and C.5.8.2. The contractor shall work with the Army Networthiness Directorate of the NETCOM 9th SC(A) to identify and resolve issues and will provide recommendations to Government. All completed actions and status for this task and sub- tasks shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001 under the authority of DID DI- MGMT-80227(T), due 45 days after contract award, then updates are due every 30 days thereafter. The Contractor may use his own format or modify the DOD format with the COTR's approval.

11.1 The contractor shall monitor and track the approved, denied and in progress Certificate of Networthiness using the established TACOM LCMC Tracking Repository and other Government provided tools IAW the contract Basic Contract PWS C.5.7.1 The Government will provide tools and information required to obtain access to the various progress reporting tools to the Contractor within 15 days of contract award.

11.2 The contractor shall provide an email notification to the customer identified within the completed CoN paperwork when a Certificate of Networthiness must be updated or expires. If contractor receives no response, the contractor shall notify the Government.

Task 12.0 G6 Cyber Security Technical Management: The contractor shall provide

Information Technology (IT) technical management based support and governance for the TACOM Life Cycle Management Command as it relates to protecting and defending information and information systems by ensuring confidentiality, integrity, availability, authenticity, non- repudiation and risk management services.

12.1 The Contractor shall provide technical IA expertise to the System Owners with configuration management activities related to IA and facilitate recommended solutions, IAW C.5.8. C.5.8.1, and C.5.8.2 for TACOM LCMC and Partners systems/applications list provided to the contractor within 15 days of contract award in accordance with the IA requirements and standards as regulated by AR 25-2, DODI Risk Management Framework (RMF) for DoD Information Technology (IT), DODI 8500.01 Cyber Security, and the Security Technical Implementation Guides (STIGS).

12.2 The contractor shall perform high-level systems analysis and evaluation of mission systems/applications for Department of the Army (DA) directed changes/updates to those systems, in support of Information Assurance (IA) and security, and IAW C.5.4.2 of the Basic Contract PWS. Analyses and results shall be documented in accordance with CDRL A001, under the authority of DID DI-MGMT-80227(T), due 45 days after contract award, then updates are due every 30 days thereafter. The Contractor may use his own format or modify the DOD format with the COTR's approval. The Contractor shall monitor system changes after implementation and report any compromises to IA/security/IA IAW contract Basic Contract PWS C.5.7.1.

12.3 The contractor shall provide customer support to System Owners and programmers in the Cyber Security business processes and procedures as they relate to system upgrades and changes, for TACOM LCMC AIS, in accordance with standards, regulations and processes identified within DoD and DA regulatory requirements, referenced IAW C.5.8, C.5.14, and C.5.5.

12.4 The contractor shall review customer provided documentation to determine required DISA STIGs and NSA Security Configuration Guides for TACOM LCMC customer and partners applications, IS, AIS and systems and required vulnerability updates as defined in the Basic Contract PWS C.5.8, C.5.8.1, and C.5.8.2.

12.5 The contractor shall review TACOM LCMC customers and partners compliance by utilizing the Vulnerability Management System (VMS) (where allowable) and the Team collaborating site to verify the customer has made the Department of Defense required STIGs and vulnerability updates for the contractors assigned application, information systems, AIS and systems and the supporting platform on which they reside as defined in the Basic Contract PWS C.5.2.8, C.5.3.7. System/application documentation shall be in accordance with CDRL A015, Software Documentation. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

12.6 The contractor shall review that the STIGs applied to their assigned application, information systems, AIS and systems are reviewed for accuracy and that the system

owner has executed the STIGs at a yearly interval for application level STIGs and every 6 months for Operating System STIGs as defined in the Basic Contract PWS C.5.2.8, C.5.3.7, C.5.9.4, C.5.8, C.5.8.1, and C.5.8.2. Any issues with STIG execution should be reported to the Government COTR IAW the Contractor's Monthly Report, CDRL A001, under the authority of DID DI- MGMT-80227(T), due every 30 days. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

12.7 The contractor shall ensure that IA personnel are maintaining and auditing access and log files for all TACOM LCMC and Partners systems and that authentication policies are audited for compliance with the DoD and DA regulatory requirements. Any recognized security violation must be reported in accordance with the TACOM LCMC incident response policy.

12.8 The contractor shall assist TACOM LCMC customers with the vulnerability scans process for their systems using DoD approved tools such the Army Gold Disk Scanner, Retina, and/or SCAP scanners. The contractor shall help the customer create the necessary mitigation reports based on the scan results, and inform the IAM of their findings. For vulnerabilities that cannot be closed, the contractor shall work with the IAM to assess the risk and determine whether the discovered vulnerabilities can be risk-accepted by the DAA. The contractor shall assist the IT system owners for assigned systems in maintaining a list of the DAA risk accepted vulnerabilities. The Contractor may use his/her own format or modify the DOD format with the COTR's approval.

12.9 The contractor shall participate in site assistance visit(s) when required in order to conduct security inspection, assessment, test, or IA review for an IT system or an ICAN that resides in a remote site location. All travel shall be conducted in accordance with section C.1.3.2 of the Basic PWS.

12.10 The contractor shall be familiar with the TACOM LCMC Incident Response policy, and shall be able to respond and provide guidance to the customers on the different types of incidents that include spillages, virus and malicious code incidents, hacker attacks, and technical vulnerabilities. The COTR shall provide this policy to the contractor within 10 days of contract award.

Task 13.0 G6 Cyber Security Administration: The contractor shall manage/maintain and monitor the effectiveness of the TACOM LCMC IA C&A program processes and functions as defined in the Basic Contract PWS paragraph C.5.8.1. All completed actions and status shall be reported in the Monthly Contract Progress, Status and Management Report, CDRL A001 under the authority of DID DI-MGMT-80227(T), due 45 days after contract award, then updates are due every 30 days thereafter. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

13.1 The contractor shall perform on-going reviews/assessments of the current TACOM LCMC Cyber Security Risk Management program as implemented within TACOM LCMC customers and Partners.

13.2. The contractor shall perform reviews of IT systems authorization documentation/artifacts to verify that the documentations are effective and meet the requirements of the DoD and DA regulations and standards. The contractor shall apply IA and DA knowledge to document any insufficiencies discovered as a result of this review and provide recommendations for compliancy to the customer and IAM within 30 days of review.

13.3 The contractor shall participate in TACOM LCMC IA Cyber Security team meetings and briefings to senior management regarding team projects and status and shall provide briefing charts, agendas and minutes for these meetings and briefings. These team meetings are not to be confused with DIACAP working groups. All completed actions and meeting status shall be reported in the meeting minutes, due 2 days after completion of meeting. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

13.4 The Contractor shall track, monitor and work with the customer to maintain the established TACOM LCMC Centralized C&A repository, for all TACOM LCMC and Partners' systems' Authorization approved artifacts, DIACAP documents, and technical documentation to support DOD IA directives. The contractor shall update assigned applications, IS, AIS, and subsystems status within the repository.

13.5 The contractor shall perform formal training for the system owners and related staff and IASOs with a minimum of four sessions and a maximum of twelve sessions per year. Training will provide relevant Cyber Security and Risk Management topics required to facilitate discussion and customer knowledge IAW the Basic Contract PWS paragraphs C.5.8.2 and C.5.9.2.

13.6 The contractor shall document any progress in Team's Metrics collection tool which shall be made available to him/her within 15 days of appointment. The contractor shall report on the following metrics: Systems DIACAP Accreditations, Cyber Security Awareness and Education, Certificate of Networthiness, Annual Reviews, Quarterly POAM Reviews, DAA Change Management Process, FISMA Compliance, DoD / Army organizations communication, DOD 8570.01M workforce improvement program, Group mailbox certificates, IAVA compliance, IA account validations, Spillages, Cyber-incidents, and any other IA actions listed in this task order.

13.7 The contractor shall participate in preparing, distributing and maintaining local organization IA policies, memorandums, SLAs and SOPs concerning TACOM LCMC and Partners' applications, ISs, and AISs.

13.8 The contractor shall monitor the team's group mailbox on a daily basis and take the appropriate action in accordance with the team's mailbox process. The Government will provide access to the mailbox and the documented process within 30 days of contract award.

Task 14.0 508 Compliance: The Section 508 contractor shall be responsible for organizing and supporting the implementation of Section 508 within TACOM LCMC. The Section 508 contractor is the central point of contact for information concerning accessibility issues and solutions. All completed actions and status shall be reported in the Monthly Contract Progress,

Status and Management Report, CDRL A001 under the authority of DID DI-MGMT-80227(T), due 45 days after contract award, then updates are due every 30 days thereafter. The Contractor may use his own format or modify the DOD format, with the COTR's approval.

- a. Establish and coordinate an IT Accessibility Team to assist in Section 508 compliance matters, and coordinate all reporting requirements.
 1. Develop charter to further define roles and responsibilities of the IT Accessibility Team
- b. Develop and implement TACOM LCMC accessibility policies, procedures, and best business practices.
- c. Develop and execute a Section 508 Implementation Plan.
- d. Coordinate the integration of Section 508 accessibility needs into TACOM LCMC budget, strategic, and IT capital plans.
- e. Identify current needs for accessible systems and adaptive technology (hardware/software) and identify IT deficiencies that impact the performance of persons with disabilities in both current and prospective IT systems.
- f. Support validation of accessible IT systems performance prior to deployment.
- g. Coordinate and provide sources of education and training to key personnel within the TACOM LCMC, identify available resources, and stay abreast of procurement changes to the FAR that will affect the purchase of any new equipment or software.
- h. Respond to future Department of Justice Section 508 surveys.
- i. Utilize major systems inventory and agency website inventory to provide a roadmap for required remediation efforts and training requirements.
- j. Maintain the TACOM Accessibility Portal as the authoritative source for all accessibility and Section 508- related information for TACOM LCMC
- k. Develop Section 508-compliant templates for briefings, memos, and other documentation for TACOM LCMC
- m. Establish contacts with other department/agency coordinators to share information about TACOM LCMC's implementation strategies.
- n. Participate in the Universal Access Working Group (UAWG) to share experiences and add "best practices" to the collaboration and learning website.
- o. Provide progress reports and ad hoc information to the Critical Infrastructure Protection (CIP) related to the implementation of Section 508.
- p. Conduct regular meeting with the Section 508 IT Accessibility Team.
- q. Monitor the Access Board (www.access-board.gov) and the General Services Administration (GSA) (www.section508.gov) web sites for new guidance and training opportunities.
- r. Prepare procedures for the development of requirements for promulgation by the CIO.
- s. Develop and implement methods for monitoring adherence to Section 508 policies and procedures.
- t. Develop market research procedures and methods to monitor adherence to these procedures.
- u. Coordinate with personnel and training to add disability awareness and accessibility training into agency training programs.
- v. Provide progress and ad hoc reports to the CIO.
- w. Contribute input on the CIO's Reports to the Department of Justice.
- x. Be familiar with FAR technology-specific provisions, including but not limited to:

1. Software Applications and Operating Systems (1194.21)

- 2. Web-based Intranet and Internet Information and Applications (1194.22)
- 3. Telecommunication Products (1194.23)
- 4. Video or Multimedia Products (1194.24)
- 5. Self Contained, Closed Products (1194.25)
- 6. Desktop and Portable Computers (1194.26)

y. Understand how Section 508 and related accessibility laws, regulations and standards apply to a broad range of organizational activities and business operations, including the procurement, development, maintenance, use of electronic and information technology.

z. Serve as the agency focal point for providing clear technical guidance and assistance related to Section 508.

aa. Conduct assessments and ongoing audits and provide remediation recommendations and support to ensure that the Agency's web pages, documents and applications are compliant with all required Government standards.

ab. Conduct in-depth Section 508 assessments via manual reviews and using automated test tools and assistive technologies (i.e., JAWS, WAVE, Windows-Eyes, AMP, etc.)

ac. Prepare reports concerning failures in Section 508 compliance and ways to remediate.

ad. Monitor resolution of Section 508 compliance violations.

ae. Assist project teams with understanding how Section 508 and accessibility activities fit within the project life cycles.

af. Partner with project leads and requirements analysts to help them appropriately document and deliver against requirements for Section 508 compliance.

ag. Experience conducting code reviews intended to find and mitigate vulnerabilities overlooked in the initial development phase. Responsible for performing security code reviews of application in order to identify vulnerabilities that could impact the confidentiality, integrity, or availability of systems. Ensure that the processes, procedures, and products used to produce [the software] conform to all requirements and standards specified to govern software development and align with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)

Minimum Qualifications:

E. Information Assurance Contractor Training and Certification

1. The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance and or network/system administrator functions in accordance with DOD 8570.01-M Information Assurance Workforce Improvement Program, AR 25-2, and the TACOM Warren training and certification policy. The Contractor shall meet the applicable information assurance baseline and computing environment certification requirements per position according to the following table:

Skill Set	Activity Supported	IA Baseline Certification	Comp. Env. Certification

a. Web Design & Tech Writing	Appl Mnt Spt & Dev	N/A	N/A
b. Program Manager	Project Management	N/A	N/A
c. Systems Engineer	Application Support	GSEC or Security + or SNCP or SSCP	MCTS/MCITP Windows Server 2008
d. Systems Engineer	Application Support	GSEC or Security + or SNCP or SSCP	MCTS/MCITP Windows Server 2008
e. Systems Engineer	Portal Sustainment	GSEC or Security + or SNCP or SSCP	MCTS SharePoint 2010, Configuration OR MCTS SharePoint 2010, Application Development OR MCTS SharePoint 2010, Application Development
f. SharePoint SME	SharePoint Sustainment	GSEC or Security + or SNCP or SSCP	MCTS SharePoint 2010, Configuration OR MCTS SharePoint 2010, Application Development OR MCTS SharePoint 2010, Application Development
g. Systems Engineer	Oracle/SQL DBA	GSEC or Security + or SNCP or SSCP	Oracle Certified Associate Oracle 10g or 11g
h. Systems Engineer	Asset Management	GSEC or Security + or SNCP or SSCP	MCTS/MCITP Windows Server 2008
i. Systems Engineer	Oracle/SQL DBA	GSEC or Security+ or SNCP or SSCP	MCTS SQL Server 2008, MCSA SQL Server 2008 (At least two of the three exams), MCSA SQL Server 2012 (At least two of the three exams)
j. Software Architect	Cyber Security	One of the following: CISSP, CISM, CAP or GLSC	N/A

k. Systems Engineer	Application Support	N/A	N/A
l. Software Architect	508 Compliance	N/A	N/A

2. The Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions to the Government for the tracking of compliant personnel.

3. Contractor personnel who do not have proper and current certifications will have privileges removed for the purpose of performing administrator or privileged user functions.

4. The contractor shall have comprehensive knowledge and ability to accurately apply knowledge of National, DOD and DA regulatory policies as defined in the Contract PWSC.5.8, C.5.2.12, relating to IA as follows: AR 25-1, AR 25-2, DODI 8510.01 DOD Risk Management Framework (RMF) for DoD Information Technology (IT), DODD 8500.01 CyberSecurity, Army Best Business Practices (BBPs), PAM 25-1-2 IT Contingency Planning, Certificate of Networthiness (CoN) Application, System and Test CoN checklists, FISMA Reporting Requirements, Army Information Technology Portfolio Management Guide (ITpfm), DISA Security Technical Implementation Guides (STIGS), Army Portfolio Management Solution (APMS), DoDD 5000.2 Defense Acquisition System, DoDI 5000.2 Defense Acquisition System instruction, IAVA, applicable NSA Security Configuration Guides, NIST Special Publications, and Federal Information Processing Standards (FIPS). The Contractor shall be knowledgeable in Government Communications Security (COMSEC), Public Key infrastructure (PKI) and AR 380-5.

F. Meetings: The Contractor shall attend status meetings with the Government and NEC Personnel, at the US Army Garrison- Detroit Arsenal, Warren, MI or by tele-video conferencing or audio- conferencing, IAW C.1.17, C.1.17.2 & C.1.17.8 of the Basic Contract PWS.

1. The Contractor shall provide updated status on contract tasks, schedules, budget, GFP, GFI, and problems/issues using the Project Planning Chart, in accordance with CDRL A005 and DIDS DI- MGMT- 80507A. The first Project Planning chart shall be provided to the Government COTR within forty- five (45) days after contract award, with subsequent updates every 30 days thereafter. The Contractor shall update the Project Planning Chart on a monthly basis in conjunction with the Project meetings.

2. Briefings: The contractor PM shall develop and present quarterly IPR (In Process Review) briefings to the Government for the task orders assigned to the PM. IPR briefings shall be scheduled by the Government on a quarterly basis. The contractor PM shall present the briefing using PowerPoint; and provide a hard copy of the slides to the leadership in attendance. The contractor shall include the following components in all briefings:

- a. Objective
- b. Attendees
- c. Project List
- d. Financial synopsis with burn rate and estimated funding at task order completion
- e. Individual project review quad charts: Milestones, Highlights, Risks & Issues, Work in Progress
- f. Summary Snapshot
- g. Questions

3. Meetings: The contractor PM shall attend status meetings regarding the CIO/G6, PEO GCS, ILSC and TARDEC task orders on the contract; meetings shall be conducted at the US Army Garrison- Detroit Arsenal, Warren, MI.

a. The first project meeting shall be held forty-five (45) days after contract award, with subsequent bi-weekly meetings thereafter. The contractor shall present a status briefing on the work that has been performed within the previous 30 days. Any results/data found during the previous 30 day reporting period shall be included in the subsequent meeting. These meetings will be facilitated by the COTR and will be scheduled on the same day and time bi-weekly. The contractor shall facilitate and attend meetings in accordance with Section C.1.17, C.1.17.2 & C.1.17.8 of the PWS.

Travel: All travel shall be conducted in accordance with section C.1.3.2 of the Basic PWS. Before traveling, the Contractor shall submit his estimated travel expenses to the COR for approval. All travel shall be in accordance with the DOD JTR.

a. Two (2) trips to Watervliet Arsenal (WVA), New York for two (2) people at approximately \$9,784/person. Duration of the trip shall be no more than six weeks. Purpose: Assist WVA with DOD Command Cyber Readiness Inspection (CCRI). Total cost: \$19,568.32.

H. Place of Performance: USAG-DTA, 6501 E. 11 Mile Rd, Warren, MI, 48397 and Selfridge ANG Base, Mt Clemens, MI.

I. Duty Hours:

1. Contractors will work the fixed traditional full-time work schedule Monday through Friday (except for designated Federal holidays and the Friday after Thanksgiving) with a basic workday of 8-hours. A predetermined report time must be no earlier than 0600 and no later than 0900. The basic work requirement will be 8.5 hours to include a mandatory 30-minute lunch break. Earlier or later start times may be requested if needed to support mission requirements IAW the PWS C.1.9.1. and will be approved by the COTR. The Government will not be responsible for any costs incurred by the contractor for the duration of any shutdown or closure unless specifically approved by the Contracting Officer in advance of the occurrence. Special requirements may present a need for alternate work schedules, for periods of time, due to maintenance or other server administration actions.

2. The Contractor shall respond to afterhours work as defined in the Base Contract C.1.9.4 & C.1.9.5. The COR/COTR shall direct this work in response to emergencies, outages, planned upgrades or system maintenance that must be completed outside of normal duty hours.

3. Ad-hoc Telework: Ad-hoc telework may be allowed on an as needed basis. Determination whether telework is allowable will depend on the requirements of the task order, and will require approval from the contract COTR in advance of the expected work. At any time the COTR can determine that ad-hoc telework is no longer needed for a specific position on a task order and will notify the contractor PM of such changes. Ad-hoc telework will be performed offsite at a contractor approved facility.

SECTION C - DESCRIPTIONS AND SPECIFICATIONS

The following have been deleted:

PERFORMANCE WORK STATEMENT

SECTION E - INSPECTION AND ACCEPTANCE

The following Acceptance/Inspection Schedule was added for SUBCLIN 4000AH:

INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
Destination	Government	Destination	Government

The following Acceptance/Inspection Schedule was added for SUBCLIN 4000AJ:

INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
Destination	Government	Destination	Government

SECTION G - CONTRACT ADMINISTRATION DATA

Accounting and Appropriation

Summary for the Payment Office

As a result of this modification, the total funded amount for this document was increased by \$ from \$ to \$2,708,358.38.

SUBCLIN 4000AH:

Funding on SUBCLIN 4000AH is initiated as follows:

ACRN: AH

CIN: GFEB001066009100010

Acctng Data: 0212015201520200000443435252 A.0021615.4.3.3.7 6100.9000021001

Increase: \$

Total: \$

Cost Code: A5XGH

SUBCLIN 4000AJ:

Funding on SUBCLIN 4000AJ is initiated as follows:

ACRN: AJ

CIN: GFEB001065783800001

Acctng Data: 02120152015202000001121232520030004537

6100.9000021001

Increase: \$

Total: \$

Cost Code: A60EE

(End of Summary of Changes)