

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. CONTRACT ID CODE	PAGE OF PAGES	
			J	1	10
2. AMENDMENT/MODIFICATION NO. 02	3. EFFECTIVE DATE 17-Jul-2014	4. REQUISITION/PURCHASE REQ. NO. 0010408407		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/MS 350 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 48063-4646			9A. AMENDMENT OF SOLICITATION NO.		
			9B. DATED (SEE ITEM 11)		
			X	10A. MOD. OF CONTRACT/ORDER NO. W56HZV-11-D-L555-T024	
			X	10B. DATED (SEE ITEM 13) 25-Sep-2013	
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)					
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/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: baysm14529 Modification: 02 to W56HZV-11-D-L555-T024 Reference Purchase Request: N/A The purpose of this modification is the following: 1. Section C- Paragraph I, number 2 of the Performance Work Statement has been added to include language regarding Ad-Hoc Telework requirements IAW paragraph C.1.7.3. of the base contract. 2. Modification 01 was incorrectly described as modification 02 in block 14 of modification 01. 3. The Total Cost of the Task Order remains unchanged. All other terms and conditions, other than those addressed in this modification, remain 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) LYNN M. BYRNE / CONTRACTING OFFICER TEL: 586-282-6553 EMAIL: lynn.m.byrne.civ@mail.mil		
15B. CONTRACTOR/OFFEROR		15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY <u>Lynn M. Byrne</u>		16C. DATE SIGNED 17-Jul-2014
(Signature of person authorized to sign)			(Signature of Contracting Officer)		

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION SF 30 - BLOCK 14 CONTINUATION PAGE

The following have been modified:

PERFORMANCE WORK STATEMENT

Section C - Descriptions and Specifications

TACOM LCMC CIO/G6 Cyber Security Office

A. Purpose: The purpose of this task order, Contract number W56HZV-11-D-L555 is to add labor hours and funding to the IT Services Contract for G6.

1. The Cyber Security Team has a requirement to provide TACOM LCMC customers and partners with the support needed to implement their information assurance requirements thereby enabling execution of the TACOM LCMC mission despite dynamic and changing DoD and DA level guidance. This support includes DoD Information Assurance Risk Management Model (Currently DIACAP), the Certificate of Networthiness (CoN) process, and cyber security Administrative and operational governance services in support of DoD and Army IA regulations.

2. 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.

3. The objective of this task is to support and maintain the DoD and DA Information Assurance policy, mandates, and procedures for implementing the Army Information Assurance 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 TACOM LCMC and Partners.

B. Skill Sets and Labor Hours by Project:

1. Skill Sets	Est. Hours	Cost/Hour	Total Costs	Mission	Task #s
Software Architect	3840	\$83.23	\$319,603.20	CYBER SECURITY	1.0-4.0

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 DIACAP IMPLEMENTATION AND SUPPORT: The contractor shall disseminate and support the CIO/G6 DIACAP 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 partially implemented DIACAP and the various DIACAP phases 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.

1.1 The contractor shall perform working group sessions with system owners to discuss current status, analyze the issue from an Information Assurance, IA, 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 publications, and the Committee on National Security Systems Information Assurance 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 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.

1.2 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 process. 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 DIACAP process and the TACOM LCMC Templates, administering and guiding System Owners through the process to include a review of completed DIACAP 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.

1.3 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 will 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 contractors 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.

1.4 The contractor shall monitor and track the System Owners' progress towards C&A within the DIACAP Process, 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 and the Systems/Networks Approval Process (SNAP) IAW the contract Basic Contract PWS C.5.7.1. The contractor will provide email notification alerts to the System Owner and the TACOM IA Cyber Security Team when accreditation documentation must be updated or expires at an interval of 6 months prior, 3 months prior, 2 months prior, 1 month prior and at expiration. 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.

1.5 The contractor shall perform quarterly reviews of DIACAP documentation/artifacts to verify that their assigned applications, IS, AIS and 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 applications within 15 days of contract award and will update quarterly as required. The contractor shall document any gaps between DIACAP 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.

1.6 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 2.0 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.

2.1 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.

2.2 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 3.0 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.

3.1 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 8510.1 DOD Information Assurance Certification and Accreditation Process (DIACAP), DODI 8500.1 Information Assurance, DODI 8500.2 Information Assurance (IA) Implementation and the Security Technical Implementation Guides (STIGS).

3.2 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.

3.3 The contractor shall provide customer support to System Owners and programmers in the DIACAP 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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 and Retina Scanner. 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 maintain a list of the DAA risk accepted vulnerabilities through the datasheet that the COTR is to provide within 15 days of appointment.

3.9 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.1.7.7 of the Basic PWS.

3.10 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 will provide this policy to the contractor within 10 days of contract award.

Task 4.0 G6 Information Assurance (IA) 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.

4.1 The contractor shall perform on-going reviews/assessments of the current TACOM LCMC IA C&A program as implemented within TACOM LCMC customers and Partners.

4.2. The contractor shall perform reviews of C&A documentation/artifacts to verify that the documentation 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.

4.3 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 meeting and briefings. These team meetings are not to be confused with DIACAP working groups. Team meetings where the contractor is required to provide a briefing or related documentation will not exceed three times per week or a total of 5 work hours. 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.

4.4 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' C&A 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.

4.5 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 IA and C&A topics required to facilitate discussion and customer knowledge IAW the Basic Contract PWS paragraphs C.5.8.2 and C.5.9.2.

4.6 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 contactor shall report on the following metrics: Systems DIACAP Accreditations, IA C&A 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.

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

4.8 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.

E. INFORMATION ASSURANCE CONTRACTOR TRAINING & CERTIFICATIONS:

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. Training Certificate or C.E. Certification
Software Architect	Cyber Security	One of the following: CISSP, CISM, CAP or GSLC	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 PWS C.5.8, C.5.2.12, relating to IA as follows: AR 25-1, AR 25-2, DODI 8510.1 DOD Information Assurance Certification and Accreditation Process (DIACAP), DODD 8500.1 Information Assurance, DODI 8500.2 Information Assurance (IA) Implementation, 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 (IT pfm), 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, patch management and all regulations and standards referenced within DoDI 8500.2, 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 at the US Army Garrison- Detroit Arsenal, Warren, MI or by tele-video conferencing or audio-conferencing, IAW C.1.17-C.1.17.8 of the Basic Contract PWS.

G. TRAVEL: All travel shall be conducted in accordance with section C.1.7.7 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.

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. 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 incurrence. Special requirements may present a need for alternate work schedules, for periods of time, due to maintenance or other server administration actions.

2. 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.

(End of Summary of Changes)