SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS *OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30.*			1. REQUISITION NUMBER A2474104I	PAGES 1 OF (2) PAGE(S)
2. CONTRACT NO GS00Q09BGD0015	3. AWARD EFFECTIVE DATE 09/29/2015	4. ORDER NUMBER GSQ115BJ0053	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
7. FOR SOLICITATION INFORMATION CALL:	a. NAME:		b. TELEPHONE NUMBER *(No Collect Calls)*	8. OFFER DUE DATE/ LOCAL TIME

9. ISSUED BY GSA Region 11 Marion Williams 301 7th Street, SW Washington, DC 20407-0000 United States (202) 708-6100	10. THIS ACQUISITION IS ☐ UNRESTRICTED ☐ SET ASIDE: % FOR ☐ SMALL BUSINESS ☐ HUB/ONE SMALL BUSINESS ☐ 8(A) NAICS: SIC: SIZE STANDARD:	11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED Destination ☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) 13b. RATING 14. METHOD OF SOLICITATION	12. DISCOUNT TERMS NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS
15. DELIVER TO Brendan L. Davis 109 Army Pentagon Room 3E334 Washington, DC 20310 United States (703) 693-2917	16. ADMINISTERED BY Marion Williams (202) 708-6100		
17a. CONTRACTOR/ OFFEROR GSI Contracts AT&T GOVERNMENT SOLUTIONS, INC. 1900 GALLOWS RD STE 105 VIENNA, VA 22182-3865 United States (703) 506-5842	18a. PAYMENT WILL BE MADE BY General Services Administration (FUND) The contractor shall follow these Invoice Submission Instructions. The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the appropriate order, and creating the invoice for that order. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).		
17b. ☐ CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER	18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED		

19. ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
ITEM NO.	TASK ITEM DESCRIPTION		PREVIOUS MOD AMT	MOD CHANGE AMT	NEW MOD AMT
0001	Base Period FFP Tasks		(b)	(b) (4)	(b) (4)

This award is in support of the Department of the Army Office of the Assistant Secretary of the Army Financial and Management Comptroller to provide IT support services. AT&T's technical and price proposals dated 07/27/2015, submitted in response to solicitation ID11150013, are accepted as to all items.

The base period of performance is September 29, 2015 through June 30, 2016. The total period of performance is a base period with four (4) 12-month options.

Base Period - 09/29/2015 - 06/30/201(b) (4)
Option Year 1- 07/01/2016 - 06/30/2017(b) (4)
Option Year 2 - 07/01/2017 - 06/30/201(b) (4)
Option Year 3 - 07/01/2018 - 06/30/201(b) (4)
Option Year 4 - 07/01/2019 06/30/2020(b) (4)
TOTAL $10,623,841.00, if all options are exercised.

The Base Period is fully funded in the amount o(b) (4)

25. ACCOUNTING AND APPROPRIATION DATA 299X . A11VR111 . F1 . 25 . C01 . H08 . . .	26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* (b) (4)

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 and 52.212-5 ARE ATTACHED. ADDENDA: ATTACHED

☑ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA: N/ATTACHED.

28. CONTRACTOR IS NOT REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. ☐ CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.	29. AWARD OF CONTRACT: REFERENCE OFFER DATE , YOUR OFFER ON SOLICITATION (BLOCK 5) INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR		31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)* Marion Williams	
30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)* Marion Williams (202) 708-6100	31c. DATE SIGNED 09/29/2015
32a. QUANTITY IN COLUMN 21 HAS BEEN Accepted and conforms to the contract as noted		32b. SIGNATURE OF AUTHORIZED GOVT. REPRESENTATIVE	32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	
37. CHECK NUMBER		38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*		
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER GSA Finance Customer Support 816-926-7287	41c. DATE	42b. RECEIVED AT *(Location)*		
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS	
AUTHORIZED FOR LOCAL REPRODUCTION		SEE REVERSE SIDE FOR OMB CONTROL NUMBER AND PAPERWORK BURDEN STATEMENT	STANDARD FORM 1449 (REV. 4/2002) Prescribed by GSA - FAR (48 CFR) 53.212	

The Section numbers in this Task Order Request (TOR) and resulting Task Order (TO) are in accordance with the Section numbers in the Alliant contract. Section C of the contractor's Alliant contract is applicable to this TOR/TO and is hereby incorporated by reference. In addition, the following applies:

C.1 BACKGROUND

The Office of the Assistant Secretary of the Army (Financial Management & Comptroller) (hereafter referred to as (FM&C)) requires contractor IT support to assist with its mission to provide financial information management services for its customers. IT support services required include: (1) DoD certification and accreditation of financial management business applications and the servers that host these applications; (2) business application and server troubleshooting, maintenance, and modernization; (3) VTC session support; (4) VIP desktop support; (5) maintenance, development and enhancements to OASA (FM&C's) public and private internet web portals; and (6) administration of internal and external Microsoft Sharepoint sites hosted on servers managed by other agencies.

The US Army Information Technology Agency (USAITA) is chartered as the IT Service Provider for Headquarters, Department of the Army (HQDA) Staff, and its Enterprise Information and Mission Assurance (EIMA) Division is the Designated Approval Authority (DAA) for the networks utilized by OASA (FM&C) personnel. USAITA's Customer Care (CC) Division functions as the Directorate of Information Management (DOIM) for HQDA Staff, and governs the administration of the classified and unclassified networks to which OASA (FM&C) users are connected. OASA (FM&C) IT support services personnel shall abide by the DOIM's authority to operate the classified and unclassified networks utilized by OASA (FM&C) personnel. As such, OASA (FM&C) IT support services personnel are expected to coordinate closely with USAITA service centers (e.g. CC, EIMA, et al) in addition to providing direct support to OASA (FM&C) personnel.

OASA (FM&C) IT Support personnel provide support to all OASA (FM&C)-managed business applications, servers, VTC units, Sharepoint sites, and web portals. The IT Support personnel ensure the timely, effective, and efficient delivery of information system support to OASA (FM&C) personnel. OASA (FM&C) "Information Systems" (IS)

are defined as the collection of servers, desktops, laptops, VTC equipment, web portals, Sharepoint sites, and business application software owned and operated by the OASA (FM&C). The total inventory of information systems includes 525 desktops/laptops, 23 servers, 7 VTC units, one public web portal, one internal web portal, one agency Sharepoint site on a server hosted by USAITA, one Sharepoint site hosted on a server hosted by DISA, and 11 OASA (FM&C)-unique business applications. All supported servers, desktops and laptops use the Microsoft Windows platform.

C.1.1 AGENCY MISSION

To provide timely and robust support for development, operations and maintenance of critical applications software and corresponding hardware platforms used by the Army's world-wide financial community.

C.2 SCOPE

OASA (FM&C) IT Support Services required by the contractor fall into three broad categories: 1) tasks that support the sustainment of a robust operational environment, 2) tasks that facilitate Information Assurance, and 3) tasks that facilitate VTC communications.

C.3 CURRENT ENVIRONMENT

C.3.1 Servers and Hardware:

Compaq DL580 G2: 1

Compaq DL580 G7: 1

SpectraLogic T50e Tape Backup Server: 1

IBM LS20 Blade Server: 16

IBM LS22 Blade Server: 4

IBM HS22 Blade Server: 8

Virtual Hosts: qty=8 VM ESX 5.5

Virtual Servers: qty=34 ESX 5.5

C.3.2 Server Software:

Windows 2008, Windows 2008R2, (Windows 2012R2 coming soon)

ESX 5.5

vCenter 5.5

SQL 2005, SQL 2008R2, SQL 2012

SQL Clustering

SQL Reporting Services

Microsoft Terminal Services

IIS 6

IIS 7.5

Backup Exec 2010

Event Sentry 3.1

Attachmate File Xpress Gateway

Directory Report

Application License Managers (for SPSS, Minitab, QC3, and @Risk)

C.3.3 Financial Management Applications:

www.irmis.army.mil : AT&T-developed financial information system

www.irmistraining.army.mil: AT&T-developed financial information training system

www.cmics.army.mil : AT&T-developed financial information system

www.cre.army.mil : AT&T-developed financial information system

www.eas.army.mil : CACI-developed financial information system

www.asars.army.mil : CACI-developed financial information system

www.ppbe.army.mil : CACI-developed financial information system

www.asafm.army.mil : Internet site

https://fmnet.hqda.pentagon.mil : Intranet site

http://fmwebdav.hqda.pentagon.mil : File transfer support used for receiving financial data from various sources. Also primary transfer method for moving code by the developers

https://ecss.hqda.pentagon.mil/agencies/asafm: Internal Sharepoint Site Collection hosted on USAITA server

NOTE: Link being developed - External OASA (FM&C) Sharepoint Site Collection hosted on DISA server.

C.3.4 Non-Standard COTS/GOTS Software:

These software applications are not part of the Standard image provided by IMCEN. These software applications are managed and maintained by the OASA (FM&C) IT Support contractor:

SEER

ACEIT

Cognos Improptu

SPSS

ACM

MIAP

FCM

MiniTab

ODBC connections to IRMIS/DAQS/ODS

Price True Planning

QSM-Slim

@Risk

Oracle Runtimes and Instant Clients

JMP

Camtasia

SnagIt

iGrafx

C.3.5 VTC Equipment

The primary VTC CODEC is located in the Pentagon, Room 3C349. There are also two VTC CODECs located in Ft. Belvoir Bldg 216, one VTC CODEC located in Pentagon 3D349, one VTC CODEC located in Pentagon 3E352, one VTC CODEC located in Pentagon 3B349, and one VTC CODEC located in Polk 900. All of the VTC CODECs operate at the unclassified level, with the exception of one CODEC at Ft. Belvoir Bldg 216.

C.3.6 LOCATIONS AND USERS SUPPORTED

As of May 2015, the number and location of OASA (FM&C) customers currently supported within the Washington, D.C. Metropolitan area are as follows:

OASA (FM&C) Location	Approximate No. of Users
Pentagon	370
Fort Belvoir Bldg 216	50
Polk Bldg [Crystal City]	60
Hoffman Building [Alexandria]	80

C.5 OBJECTIVES

The objective of this task order is to acquire the necessary IT Services to support all OASA (FM&C)-managed servers, VTC CODECs, business applications, Sharepoint sites, and web portals. The supported server inventory consists of 23 servers. The supported user community consists of approximately 570 individual registered system users. Support will be limited to approximately 510 user workstations (used by contractors who have been issued Government computers) in order to ensure the operability of OASA (FM&C) business applications. The primary provider of desktop support for this group of users is the USAITA helpdesk. Robust desktop support of approximately 60 VIPs is provided in order to minimize VIP downtime. For the purposes of this task order, "VIPs" are defined as personnel with civilian rank of GS-15 and above and military rank of O6 and above. IT support services personnel are granted privileged access to classified and unclassified OASA (FM&C) Information Systems (servers, desktops, laptops and business application software) in order to perform troubleshooting, maintenance, and customer support for the systems under their purview. No network devices such as routers or switches are included. There is one public facing website, one internal website, one internal Sharepoint site (hosted on an USAITA server), and one external Sharepoint site (hosted on a DISA server).

C.6 TASKS

C.6.1 TASK 1 – ACCOUNTING FOR CONTRACT SERVICES

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collections site where the contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this task order. The contractor is required to completely fill in all the information in the format using the following web address https://cmra.army.mil. The required information includes:

1. Contracting Office, Contracting Officer, Contracting Officer's Representative
2. Contract number, including task and delivery order number
3. Beginning and ending dates covered by reporting period
4. Contractor name, address, phone number, e-mail address, identity of contractor employee entering data
5. Estimated direct labor hours (including subcontractors)
6. Estimated direct labor dollars paid this reporting period (including subcontractors)
7. Total payments (including subcontractors)
8. Predominant Federal Service Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each subcontractor if different)
9. Estimated data collection costs
10. Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army requiring Activity is responsible for –providing the contractor with its UIC for the purposes of reporting this information.
11. Locations where contractor and subcontractor perform the work (specified by zip

code in the United States and nearest city, country, when in an overseas locations, using standardized nomenclature on website

12. Presence of deployment or contingency contract language
13. Number of contractor and subcontractor employees deployed in theater this Reporting Period (by country).

As part of its submission, the contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance, not to exceed 12 months ending September 30 of each government fiscal year and must be reported by 31 October of each calendar year. Contractors may use XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

The costs to be reported under this CLIN are those associated with the reporting requirements specified in Description/Specification/Statement of Work. The costs reported are those that relate to this task order only.

C.6.2 TASK 2 - TASK ORDER PROGRAM MANAGEMENT

The contractor shall provide all necessary personnel, material, equipment, administrative, financial, and managerial resources necessary for the support of this task order.

The contractor shall participate in a Government-scheduled Kick-Off Meeting after task order award. Key prime contractor and any subcontractor personnel shall participate in the Kick-Off Meeting. The purpose of this Kick-Off Meeting is to (1) aid both the Government and contractor personnel in achieving a clear and mutual understanding of all requirements, and (2) identify and resolve potential problems. The contractor shall

be prepared to discuss any issues requiring clarification and gather information necessary for the Project Management Plan and Transition Plan.

The Kick-Off Meeting shall include, but not be limited to, the following topics:

- Program Review
- Existing and Planned Applications and Technical Initiatives
- Personnel and Physical Security Issues

The Government and contractor will schedule the Kick-Off Meeting. It is anticipated that the Kick-Off Meeting will be NLT 5 working days after task order award. The contractor shall begin preparation of the Updated Transition Plan Immediately following successful completion of the Kick-Off Meeting.

C.6.2.1 - PROJECT MANAGEMENT PLAN

The contractor shall develop and maintain throughout the task order period of performance, a Project Management Plan (PMP) that shall be used as a foundation for information and resource management planning. The contractor shall deliver the PMP to the Government within 15 work days after Task Order award.

The PMP shall include, but not be limited to, the following:

- Status of current and planned tasks and subtasks
- Base schedule overlaid with actual schedules, for each task
- Project Organization
- Project Transition Processes and Schedule
- Work Breakdown Structure (WBS)

- Process Management and Control
- Overall Organizational Structure
- Project Responsibilities to include process flowcharts for all major tasks
- Task dependencies and interrelationships
- Contractor personnel assignments and duration (Staffing Plan)
- Updated Deliverable Schedule (based on solution)
- Deliverables (draft, interim, final, etc.),
- Contingency Plans (where appropriate),
- Contractor travel information
- Quality Control plan
- Risk Management plan
- Subcontract Management (organization of personnel, software and hardware)
- Monitoring mechanisms including Program Metrics
- Automated Tools, Techniques, and Methods

The contractor shall keep the PMP up-to-date, be accessible electronically at any time, and be prepared to brief any PMP content to the Government at short notice (within 24 hours). The PMP shall be used as a foundation for the Status Report.

C.6.2.2 START-UP SERVICE PLANS

The Contractor shall develop a Service Level Management Process, Scheduled Progress Reports, and Briefings. Section F.5 shows the delivery schedule for these start-up service plans.

C.6.2.3 SERVICE LEVEL AGREEMENTS (SLAs)

The Contractor, in coordination with OASA (FM&C) as its customer, shall develop SLAs for all IT Services being provided under the IT Support Services Support contract.

C.6.2.4 SERVICE LEVEL MANAGEMENT

Service Level Management (SLM) is essential in any organization so that the level of IT Service needed to support the business can be determined, and monitoring can be initiated to identify whether the required service levels are being achieved - and if not, why not. Service Level Agreements (SLAs), which are managed through the SLM process, provide specific targets against which the performance of the support services vendor can be judged.

The SLM process shall include the Contractor's plan, provision, performance, improvement and assignment of key elements of each phase in the management life cycle. The Contractor shall identify any SLM tools or software they require to implement the SLM program.

C.6.2.5 SERVICE LEVEL MANAGEMENT PROCESS

The Contractor shall be responsible for the Service Level Management (SLM) process that addresses the entire life cycle of a service, from the implementation of the service to the retirement of the service. The Contractor shall be directly responsible for scheduling, tracking, risk analysis, cost management, variances, change management, and evaluating the performance of personnel assigned to perform services on this Task Order. The Contractor shall be responsible for ensuring resources are provided that are capable of performing administrative support functions commensurate with the Task Order staffing levels. Examples of administrative support functions include, but are not limited to, information dissemination to staff members, preparation of monthly progress reports, data entry, property accountability, employee work schedules, phone rosters, briefing preparations, meeting minutes, meeting agendas, responses to data calls, and like activities.

C.6.2.6 MONTHLY PROGRESS REPORTS

The Contractor shall conduct monthly In-Progress Reviews (IPR) as agreed to at the Task Order Kick-Off meeting. The Contractor shall prepare and deliver the monthly progress report on the 15th of each month, 24 hours prior to the scheduled meeting. The IPR shall discuss at a minimum the following topics:

- Agenda/Task Review and schedule/Action Items Past and Future
- Review by Task
- Schedule by Task
- Previous Month's Activities by task
- Planned Activities for next month by task
- Issues
- Actions required by OASA (FM&C)
- Summary

C.6.2.7 BRIEFINGS

The Contractor shall be required to prepare and present briefings to the Government on the results of efforts undertaken under this Task Order.

C.6.2.8 QUALITY ASSURANCE

The Contractor shall develop, implement, and maintain a Quality Control Plan (QCP) and provide annual updates. The Contractor shall define a process that supports the execution of the tasks delineated in this PWS. The plan shall include inspection, validation, evaluation, corrective action and procedures necessary to affect quality control of all performance and products under this task order in accordance with Quality Assurance Surveillance Plan (QASP) The system shall allow inspection and evaluation

by the Government. The system shall be applicable to all subcontractors and members of the Contractor's team, if appropriate.

The contractor shall ensure the quality of products and services delivered under this task order. The contractor shall apply industry standard and best practices quality assurance practices in program management to include, at a minimum, identification of quality control factors and processes, evaluation methods, performance monitoring and process improvement.

The contractor shall prepare a Quality Control Plan (QCP) documenting its quality assurance program for approval by the Government and shall perform quality assurance in accordance with the QCP.

C.6.3 TASK 3 - INFORMATION TECHNOLOGY SUPPORT

C.6.3.1 APPLICATION SOFTWARE SUPPORT

The Contractor shall provide Information Technology (IT) support to the OASA (FM&C) user community covered by this PWS. The required IT support includes, but is not limited to:

(a) Identify, troubleshoot, implement and resolve OASA (FM&C) application software issues on OASA (FM&C) clients and on servers hosted by USAITA OPS. Typically, a user will call the OASA (FM&C) Information Management Office with a problem, and IT support personnel will document and track the issue from initial call-in to final resolution. The contractor shall troubleshoot the problem either locally, or from remote client locations. There are approximately 15 trouble calls per week on average. The current volume of trouble tickets outside the core hours of 06:00 to 18:00 is negligible.

(b) Image/Re-image OASA (FM&C) owned and managed assets. CPUs sometimes need to be re-imaged in order to upgrade them, or when responding to certain security incidents (such as classified message incidents).

(c) Install and configure business application software on user workstations. Coordinate installation of business application software on servers managed by USAITA OPS. A comprehensive list of applications used within OASA (FM&C) is provided in Sections C.3.2 and C.3.3 of this PWS.

(d) Perform hardware and software maintenance, such as: installation/replacement of motherboards, interface cards, keyboards, mice, cables, monitors, printers, and keyboard, video, or visual display unit, mouse (KVM) switches. Typical user problems include account lockouts, insufficient permissions, hard drive failures, data restoration requests, software misconfiguration, slow response time, conflicts between the business application and the underlying OS, and unfamiliarity with business applications.

(e) Provide customer assistance support in setting up user workstations and installing authorized business applications.

User Support Requirements: The Contractor shall develop a "triage" approach to user support such that VIP users have priority over general users, and issues impacting the most users have priority over issues impacting the fewest users. The Contractor shall constantly monitor his/her trouble ticket queue, and will call the customer within 2 hours of trouble ticket report receipt. The Contractor shall provide the user with an estimated time of when response to the problem can be initiated. If the response cannot be initiated within 1 business day (due to current backlog), the Contractor shall inform the Government lead, who will then either adjust the technician's work queue, or will interface with the customer to explain the delay. The Contractor shall NOT resolve issues by telling the customer to call another division/entity to request assistance for resolving an IT issue that falls within the scope of this PWS. The Contractor shall make all calls/coordination necessary to resolve IT issues as part of the responsibility to fully manage resolution of the issue. The triage support is for software and hardware, however, over 90% of all issues are software related. Triage describes an approach by which Contractor shall sort out who gets taken care of first, and/or which issue gets taken care of first in event that there are multiple customers and/or issues to take care of at the same time.

C.6.3.2 SERVER ADMINISTRATION SUPPORT

The Contractor shall act as the Server Administrator for the OASA (FM&C) owned and managed servers listed in C.3.1 to the PWS. Server administration tasks include, but are not limited to:

(a) Identify, troubleshoot, and resolve (or manage the resolution of) application software, operating systems, hardware, and network performance issues on OASA (FM&C) owned and managed servers. Server problems will not always be self-evident, and will often be discovered when troubleshooting user issues. System Administrators are expected to constantly monitor server performance in order to stay on top of problems before they turn into major outage events.

(b) Perform problem analysis and systems monitoring for OASA (FM&C) owned and managed assets. The Contractor shall conform to well-established best practices in the art of server administration to ensure the sustained robust performance of OASA (FM&C) owned and managed servers. The Contractor shall have solid familiarity with all appropriate DISA STIGs, and will use them as a primary source for server configuration guidance.

(c) Recommend system design, configuration, and administration control procedures to enhance systems performance. All procedures will be documented and submitted to the Government lead.

(d) Assist in resolving system architecture issues, including hardware configurations and interconnections

(e) Monitor activity, growth, and performance of database, file, print, and web servers in order to make recommendations for improvement.

(f) Document all significant server actions taken, and incorporate these actions into a monthly status report provided to the Government leads. Actions that should be documented include service packs applied, hot fixes applied, and server anomalies of interest.

(g) Research, acquire, track, test, and implement OS and application software upgrades, security patches, and hot fixes. Generally speaking, it is a server administration best practice to ensure that all servers are completely up-to-date with the latest patches, hot fixes, and software versions. The Contractor shall adhere to guidance issued by the JTF-GNO (through IAVMs and assorted other directives), DISA, IMCEN, and the Government Lead on various actions that must be undertaken to achieve optimal server functionality and security.

Server Administration Requirements: The Contractor shall constantly monitor and observe server performance using automated tools and established checklists. There are no prescribed tools; however OASA (FM&C) uses EventSentry. The Contractor shall install major patches and hot fixes on servers after hours or on weekends in order to achieve minimum impact to users. To be successful on this task order, the Contractor shall administrate servers with the necessary proficiency to achieve satisfactory results on all audits (both from internal sources and external sources). DISA CCRI, and USAITA inspections shall reveal zero (0) previously unaccounted for Category I findings. Microsoft Windows is the server operating system for this requirement.

C.6.3.3 VTC ADMINISTRATION AND SUPPORT

The Contractor shall provide a full spectrum of VTC support services for OASA (FM&C)-owned VTC CODECs. VTC Support tasks include, but are not limited to:

(a) Facilitate the setup and launch of all VTC meetings involving OASA (FM&C) personnel with rank of O6 (GS15) or higher. Among other things, this involves coordinating with the VTC bridge and supplying the pertinent details to the bridge for the OASA (FM&C) side of the connection.

(b) Identify, troubleshoot, and resolve (or manage the resolution of) problems arising from VTC hardware and session issues. VTC problems will not always be self-evident, and will often be discovered when troubleshooting user issues. VTC Administrators are expected to constantly monitor VTC CODEC performance in order to stay on top of problems before they turn into major outage events.

(c) Act as the resident VTC subject matter expert (SME) for VTC technology. The Contractor shall have solid familiarity with the VTC equipment, and will be able to demonstrate basic use of VTC equipment to OASA (FM&C) users on request.

(d) Recommend system design, configuration, and standard operating procedures to enhance systems performance. All procedures will be documented and submitted to the Government lead.

(e) Assist in resolving system architecture issues, including hardware configurations and interconnections.

(f) Document all significant VTC actions taken, and incorporate these actions into a monthly status report provided to the Government leads. Actions that should be documented include a log of VTC sessions launched, session problems encountered, and equipment malfunctions.

(g) Research, acquire, track, test, and implement VTC firmware upgrades and pertinent security policies. The Contractor shall adhere to VTC configuration guidance issued by the DAA, CIO/G6, DISA, and the Government Lead on various actions that must be undertaken to achieve optimal VTC functionality and security.

VTC Administration and Support Requirements: The Contractor shall constantly monitor and observe VTC performance using automated tools and established checklists. There are no prescribed tools. The Contractor shall install major patches and configuration changes on VTC CODECs after hours or on weekends in order to achieve minimum impact to users. To be successful on this contract, the Contractor shall configure VTC equipment with the necessary proficiency to achieve satisfactory results on all audits (both from internal sources and external sources). DISA and USAITA inspections shall reveal zero (0) previously unaccounted for Category I or Category II findings.

C.6.3.4 VIP DESKTOP SUPPORT

The Contractor shall provide government-furnished desktop and laptop support to all agency VIPs. VIPs are defined as personnel who hold a rank of GS15 and above or O6 and above. There are approximately 55 users with such rank throughout OASA (FM&C). For desktop/laptop issues in which the contractor lacks the appropriate rights, permissions, or knowledge to effectively resolve the problem, the contractor shall interface with the USAITA Tier 2 helpdesk and/or USAITA "Gold Team" until such time that resolution is complete. Current VIP workload is approximately 50 help requests per month. It is understood that actual resolution times may vary depending on the problem. Depending on the VIP and/or the issue involved, the Government may direct contract personnel to temporarily dedicate a specific block of work hours exclusively toward problem VIP problem resolution.

VIP Desktop Support Requirements: The Contractor shall track VIP support requests on a spreadsheet designed for that purpose. The spreadsheet shall include name, date

reported, brief problem description, brief resolution description, and resolution date. 90% of VIP support requests shall be responded to within 1 hour.

C.6.3.5 LIFECYCLE SUPPORT

The Contractor shall provide equipment lifecycle replacement cost estimates to the Government Lead. Lifecycle support duties also include but are not limited to:

(a) Tracking all software and hardware licenses and warranties and providing cost data to the Government Lead.

(b) Notifying the Property Book Officer and/or Government Lead for disposition instructions when Information Systems are at their end of lifecycle. The Government Lead must be copied on all reports furnished to the PBO.

Lifecycle Support Requirements: The Contractor shall devise an inventory tracking process to track software/hardware inventories, licenses, and warranties. The inventory tracking process shall contain cost data that shall be furnished to the Government Lead for budgeting purposes.

C.6.3.6 CONFIGURATION MANAGEMENT

The Contractor shall be responsible for keeping a comprehensive record of all OASA (FM&C) procured software installed on OASA (FM&C) owned and managed hardware. The list of Government-approved software shall also track software versions and release levels. Standard Load images installed on OASA (FM&C) owned and managed hardware will also be archived and tracked. The Contractor shall remove all unauthorized software from OASA (FM&C) owned and managed hardware upon direction of the OASA (FM&C) IMO.

Configuration Management Requirements: "The contractor shall create an Excel spreadsheet that delineates non-standard-load software that is loaded onto each

workstation. Non-standard-load software is all software that is *not* provided by USAITA (the agency's network service provider)." The spreadsheet shall be keyed by user name, and delineate the name of the workstation used by that user, followed by columns indicating the non-standard-load software used by the user."

C.6.3.7 WEB PORTAL DEVELOPMENT & MAINTENTANCE

OASA (FM&C) operates internal and external web portals that together are a critical financial information resource for Army users worldwide. The portals contain a tremendous knowledge base of financial information, as well as an interactive information component. The Government will provide all web portal content. The Government will also provide information to achieve the proper function, look, and feel of the web portals.

Web Portal Development & Maintenance Requirements: The Contractor shall supply the necessary web development and webmaster expertise to re-develop and sustain the OASA (FM&C) web portals. The web portals shall consistently exhibit the function, look, and feel designated by the Government. Web portal availability shall exceed 99%, and 90% of webmaster requests shall be closed out within 2 business days.

C.6.3.8 SHAREPOINT SITE ADMINISTRATION & MAINTENTANCE

OASA (FM&C) operates two distinct Sharepoint site collections. One of these site collections is hosted on a USAITA Sharepoint Server. The other site collection is hosted by DISA as part of their Sharepoint Service. These Sharepoint site collections are comprised of many OASA FM department sites. These sites collectively form a critical financial information resource for Army users worldwide. The sites contain a tremendous knowledge base of financial information, as well as an interactive information component. The Government will provide all Sharepoint site content. The Government will also provide information to achieve the proper function, look, and feel of the Sharepoint site collections.

Sharepoint Site Collection Administration & Maintenance Requirements: The Contractor shall supply the necessary Sharepoint administration expertise to sustain the OASA (FM&C) Sharepoint site collections. The Sharepoint site collections shall consistently exhibit the function, look, and feel designated by the Government. 90% of Sharepoint administrator requests shall be closed out within 2 business days. The contractor shall interface with Sharepoint server administrators at USAITA and DISA to facilitate maximum Sharepoint site uptime.

C.6.3.9 SYSTEM BACKUPS

Regular, frequent backups are vital for the continuity of the OASA (FM&C) enterprise. To verify the efficacy of backup procedures, the Contractor shall periodically test backups by restoring backed up data in a test operational environment and verifying the integrity of the restored data.

Configuration Management Requirements: The Contractor shall perform incremental and full system backups IAW frequencies articulated by the onsite Government CTR . The Contractor shall periodically test (at least once per quarter) a system backup by restoring it in a test environment and verifying the integrity of the restored data. Integrity comparison to operational data shall be 100%. If not, backup proficiency shall be deemed unreliable, and the onus shall be on the Contractor to devise a backup procedure that yields the desired result.

C.6.4 TASK 4 - INFORMATION ASSURANCE

C.6.4.1 VULNERABILITY ASSESSMENT SUPPORT

The Contractor shall conduct monthly vulnerability assessments of all OASA (FM&C) owned and managed assets (to include web applications, business application software, and VTC systems). Contractor shall report the results to the OASA (FM&C) Information Management Officer (IMO) using the built-in reporting features of the vulnerability assessment tool, and will manage and track mitigation actions for the vulnerabilities identified in the report generated by the vulnerability assessment scan.

The Contractor shall ensure that all mitigating actions are completed within 7 working days. If mitigating actions cannot be accomplished within 7 days, the contractor shall report to the IMO the following information:

- Vulnerability Identified
- Number of vulnerable systems
- Plan to mitigate vulnerabilities and estimated time to resolution
- A daily report detailing the progress made toward mitigating the vulnerabilities identified by the monthly vulnerability scan.

Vulnerability Assessments Requirements: The Contractor shall conduct monthly vulnerability assessments and to either (a) mitigate the vulnerabilities revealed by the scans within 7 working days; or (b) submit a report to the OASA (FM&C) IMO, updated daily, detailing the progress made toward vulnerability mitigation.

C.6.4.2 MALWARE DEFENSE ASSESSMENTS

The Contractor shall conduct weekly malware defense assessments of all OASA (FM&C) owned and managed servers and laptop assets. The purpose of this assessment is to ascertain that the anti-virus definitions of OASA (FM&C) owned and managed assets are up-to-date, and that anti-virus clients are properly installed and functioning. The Contractor shall report the results to the IMO using the built-in reporting features of the Host-Based Security System (HBSS) tool, and will manage and track mitigation actions for assets with substandard anti-virus capability. The Contractor shall mitigate all identified anti-virus problems, and will ensure that all mitigating actions are completed within 7 working days. If mitigating actions cannot be accomplished within 7 days, the contractor shall submit a report to the IMO with the following information:

- Anti-Virus problem
- Number of systems subject to the problem
- Plan to fix the problem(s) and estimated time to resolution

- A daily report detailing the progress made toward fixing the problem identified by the weekly malware defense assessment.

Malware Defense Assessments Requirements: The Contractor shall conduct weekly malware defense assessment scans and mitigate anti-virus problems revealed by the scans.

C.6.4.3 INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM)

The Contractor shall ensure that all OASA (FM&C) owned and managed servers, workstations, laptops, and printers are compliant to all Information Assurance Vulnerability Management (IAVM) notices issued by the JTF-GNO. JTF-GNO IAVM notices include alerts, bulletins, and tech tips. IAVM alerts are more commonly referred to as "Information Assurance Vulnerability Alert (IAVA)'s" or simply "alerts".

C.6.4.3.1 IAVM Notice Acknowledgement

The Contractor shall keep abreast of all IAVM notices issued by the JTF-GNO. Notices are delivered through the AKO's IAVA community and via subscription to the JTF GNO's IAVA list server. All IAVM notices (alerts, bulletins, and tech tips) shall be acknowledged in the Asset & Vulnerability Tracking Resource (A&VTR) database by their specified acknowledgement due date. The A&VTR is managed by the Army CIO/G6, and is the Army's central repository for reporting IAVA compliance.

IAVM Notice Acknowledge Requirements: The contractor shall acknowledge 100% of all IAVM notices in the A&VTR database by the acknowledgement suspense date indicated in the IAVM notice.

C.6.4.3.2 IAVM Notice Compliance Verification

The Contractor shall verify that all OASA (FM&C)-managed servers, workstations, laptops,and printers conform to the security requirements mandated in IAVM notices by their respective due date.

Upon receipt and acknowledgement of each IAVM notice, the Contractor shall:

- Scan all OASA (FM&C)-managed assets for the vulnerabilities identified in the notice.
- Patch and rescan OASA (FM&C)-managed assets until they are 100% compliant to any given IAVM notice.

Information Assurance Vulnerability Alert (IAVA) Notice Compliance Verification Requirements: The contractor shall establish 100% IAVA compliance to at least 99% of the total number of assets used as the basis for a given scan. The 99% figure represents a satisfactory figure for the number of available assets (as a percentage of the number of total assets).

C.6.4.3.3 IAVM Notice Compliance Reporting

The Contractor shall report IAVM Notice compliance as follows:

- Compliance data for IAVM alerts will be reported to the Army's "Asset & Vulnerability Tracking Resource" (A&VTR) database.
- Compliance data for IAVM notices (to include alerts, bulletins, and tech tips) will Be reported to the IMO on a weekly basis using a spreadsheet devised for that purpose.

IAVM Notice Compliance Reporting Requirements: The contractor shall submit current, accurate, and complete reports every week to the IMO. A&VTR data shall likewise be kept current, accurate, and complete with respect to all IAVM alerts. To be current, data must be no more than 7 days old in the weekly IAVM compliance report, and no more than 30 days old in the A&VTR. To be accurate, data must properly reflect actual IAVA compliance for each and every asset reported. To be complete, data must reflect 100% of all assets actually scanned.

C.6.4.3.4 IAVA Plan of Action & Milestones (POA&M)

One day before the suspense date specified in a given IAVA, the Contractor shall prepare and submit an acceptable Plan of Action & Milestones (POA&M) to the A&VTR database for all IAVAs for which compliance is not yet attained.

IAVM Alert Mitigation Action Plans Requirements: The Contractor shall submit a POA&M one day before the compliance due date of every IAVA for which 100% compliance has not been attained. The extent of vulnerabilities is characterized as trivial.

C.6.4.3.5 IAVM Notice Quarterly Verification

The Contractor shall rescan all OASA (FM&C)-managed assets for all non-rescinded and non-superseded IAVM notices every quarter. The same method described in paragraph 5.2.4.4 shall be employed to conduct a quarterly re-verification of all past IAVM notices. The Contractor shall update the A&VTR with the alert compliance data obtained by conducting this quarterly scan. The contractor shall submit a quarterly report of IAVM compliance to the IMO. The report shall be in the same format as the weekly IAVA report.

IAVM Notice Quarterly Re-verification Requirements: The Contractor shall establish 100% IAVA compliance to at least 99% of the total number of assets used as the basis for the quarterly scan. The 99% figure represents a satisfactory figure for the number of available assets (as a percentage of the number of total assets).

C.6.4.4 ACCESS CONTROL

The Contractor shall:

(a) Verify that OASA (FM&C) personnel meet required security investigation, clearance, authorization, mission requirement, and supervisory approval before they are granted access to an IS.

(b) Manage and review user accounts, access permissions, and logins in order to suspend or terminate accounts IAW local policy.

Access Control Requirements: The Contractor shall validate that 100% of users requesting access to the HQDA Enterprise Network (HEN) and HQDA Classified Enterprise Network (HCEN) possess the proper qualifications for access. The Contractor shall adhere to local policies governing the termination/suspension of accounts, and the manipulation of system accounts. The Contractor shall never use privileged access to conduct work that can be performed with non-privileged access.

C.6.4.5 CERTIFICATION AND ACCREDITATION

The Contractor shall conform to DIACAP (or any successor DoD-approved C&A process) when preparing System Security Authorization Agreements (SSAAs) for Information Systems managed and/or operated by OASA (FM&C). Specific C&A requirements will be delineated by the DAA and articulated by USAITA. The Contractor shall coordinate with and solicit support from USAITA when developing, maintaining, and updating System Security Authorization Agreements (SSAAs), Certificates of Networthiness, and ATO's for OASA (FM&C) Information Systems. The Contractor shall perform a risk analysis and ensure that all requisite certification tasks are performed as required for all OASA (FM&C) information system assets. Requisite C&A documentation shall be embodied in a DAA-approved certification and accreditation tool. OASA FM&C utilizes XACTA IA Manager.

Certification & Accreditation Requirements: The Contractor shall maintain a current and accurate C&A portfolio for all OASA (FM&C) owned and managed assets, and record appropriate C&A documentation in a DAA-approved certification and accreditation tool. The accreditation of the system runs on a 3 year cycle and recertification is due annually. Typically, the reaccreditation process starts one year before the expiration of the current accreditation. The OASA requires the use of specific templates.

C.6.5 TASK 5 - COMPUTER NETWORK DEFENSE

C.6.5.1 COMPUTER SECURITY INCIDENT RESPONSE MANAGEMENT

The Contractor shall manage the resolution of all security incidents occurring on OASA (FM&C) owned and managed assets. Security Incidents are forwarded by the PENTCIRT via Questionable Activity Reports. Security incidents may also be revealed upon the required periodic review of IS security/event log files. The Contractor shall have 1 business day to investigate the incident. After 1 business day, the machine in question is blocked from the network until the IMO receives a satisfactory response to the Questionable Activity Report. In responding to security incidents, the Contractor shall:

- Document incidents in the OASA (FM&C) Security Incident Spreadsheet (SIS) within 1 hour of receipt. Tasks involved to properly document security incidents include:

- Tracking the incident in the SIS and updating the appropriate government leads As significant investigatory events occur.
- Indicating man-hour cost calculations within one business day of closing the incident.

- Collect forensic evidence related to the security incident and of any other suspect activity uncovered while investigating the security incident. Such evidence must be kept as forensically sound as possible.
- Manage or perform the resolution of each incident in accordance with PENTCIRT guidance. Security Incidents must be investigated or managed until the incident is closed. The following list describes security incident categories:

- Category 1: Unauthorized root access. This category describes incidents in which someone who should not have access has obtained root level privileges on one or more systems. The implications for this can range from very serious (we've been hacked), to false positive (technician performing unscheduled work). The Contractor shall provide the Pentagon Computer Incident Response Team (PENTCIRT) or other appointed investigators with all requested support.

- Category 2: Unauthorized user access. This category describes incidents in which someone has obtained non-privileged access to one or more systems. Again, the implications could range from serious to false positive. The Contractor shall provide PENTCIRT or other appointed investigators with all requested support.

- Category 3: Unsuccessful Activity Attempt. This category describes incidents in which someone has attempted to obtain unauthorized access to one or more systems (that, had they been successful, would have resulted in a category 1 or category 2 incident). The Contractor shall provide PENTCIRT or other appointed investigators with all requested support.

- Category 4: Denial of Service Attack. This category describes incidents in which an intruder is successful in degrading network, application, or workstation performance through some type of malicious logic. Incidents such as these typically result from a viral infection, and can emanate either from an internal source or an external source. The Contractor shall provide PENTCIRT or other appointed investigators with all requested support.

- Category 5: Non-Compliant Activity. This category describes incidents in which a user engages in any observed poor security practice such as using weak passwords, gaining privileged access via unsecured means, installing unauthorized software, or any other action in violation of the Acceptable Use Policy.

- Category 6: Reconnaissance. This category describes incidents in which a user or an intruder conducts an unauthorized probe of the system (e.g. to find out what TCP/IP ports are open on systems).

- Category 7: Malicious Logic. This category describes incidents involving self-replicating software that is viral in nature and is disseminated by attaching to or mimicking authorized or unintended computer system functions (e.g. a Trojan Horse).

- Category 8: Investigation Ongoing. This category describes incidents that do not immediately fall into one of the other categories, but are being actively investigated as an undetermined computer security incident.

- Category 9: Explained Anomaly. This category describes incidents in which a certain activity was initially deemed suspicious, but which upon further investigation was explainable (and allowable).

- Category 10: Data Spillage. This category describes any incident that involves information of a higher classification level being placed on a system accredited for a lower classification level (e.g. Secret information being placed on the Non-classified Internet Protocol Router Network (NIPRNet).

Computer Security Incident Response Requirements: The Contractor shall provide timely response in the investigation of computer security incidents. The vast majority of computer security incidents shall be resolved within 48 hours. However, the complexity of each incident dictates how long the investigation process shall reasonably take. All incidents shall be reported in the OASA (FM&C) IA SIS (or future tracking mechanism) within 1 hour of report receipt. The Contractor shall notify OASA (FM&C) Government management if any incident is not resolved within 7 business days.

C.6.5.2 LOG FILE REVIEW

The Contractor shall perform a periodic review of all security-related log files on OASA (FM&C) owned and managed information systems. The Contractor shall establish audit trails and create archives IAW local policies or as directed by ITA EIMA. Security incidents revealed by log file review shall be handled in accordance with paragraph C.6.5.1 of this PWS.

Log File Review Requirements: The Contractor shall establish a practical (automated) means to review log file data on OASA (FM&C)-managed IS's in order to expose and resolve security incidents. Server logs shall be reviewed at least once weekly. A random sample of workstation logs shall also be reviewed once weekly. 100% of security incidents generated from log file review shall be handled IAW paragraph C.6.5.1 of this PWS.

C.6.6 TASK 6 -TRANSITION SERVICES

C.6.6.1 TRANSITION PLAN

Within 10 days of Task Order award, the Contractor shall prepare and deliver an Initial Transition Plan recommending the steps necessary to migrate from existing Government and contractor operations to the newly awarded contractor operations. The plan shall be defined in detail by specific task, deliverable, and milestone to ensure an orderly and complete transition. The transition shall be executed as quickly as possible with minimum disruption to network operations and customer service. The Government will review the Initial Transition Plan, and provide comments to the Contractor that will be addressed in the Final Transition Plan. The Final Transition Plan is due within 5 days of the receipt of the Government's comments.

Within 180 days of Task Order award, the Contractor shall prepare and deliver a Transition-Out Plan that recommends the steps required to transition network

operations from the Contractor back to OASA (FM&C) and/or the follow-on service provider at the conclusion of the Task Order. This plan will include provisions for the disposition of any contractor proprietary tools that may have been installed to support network operations such that OASA (FM&C) and/or the follow-on service provider may remain fully operational up to the standards established before exit.

The Transition Plan shall address, at a minimum, the following areas:

Transition of Program Management Support and Other Personnel

Transition of Task Requirements in the task order

Asset Transfers [hardware, software, GFP]

Resource Requirements [personnel and budget]

Security Clearance Actions and Status

Transition Milestones and Timeline

Risk Mitigation Practices

C.6.6.2 TRANSITION-IN SERVICES

The successful contractor shall perform transition-in services for no longer than 14 days after kick-off meeting necessary to provide a smooth and efficient transition from the existing contractor without any interruption or degradation in any services.

The contractor (other than the incumbent) shall prepare and submit a transition plan (SEE SECTION C.7.6.1) detailing the plan, staffing, and other information necessary to seamlessly transition from the existing task order without interruption or degradation in any services.

C.6.6.3 TRANSITION-OUT SERVICES

The contractor shall perform all services necessary to transition the work performed under this task order to the Government or another contractor at the conclusion of this task order. The transition shall be performed without any interruption or degradation in any services. The contractor shall perform all transition-out services necessary to provide a smooth and efficient transition.

The Contractor shall use best commercial practice for formatting deliverables under this contract.

C.6.7 SECTION 508 COMPLIANCE

For all electronic and information technology (EIT) products and/or services supported under this task order, the Contractor shall analyze and present to the Government in a Product Accessibility Report that documents the potential accessibility challenges presented by the product and recommendations for solving them. The Contractor shall use the Government Product Accessibility Template (GPAT) as the basis for the report in order to assess any potential accessibility impact, and provide a recommended solution to remedy any potential accessibility difficulties to the Government for approval. Please see the following websites for additional information: www.section508.gov and www.buyaccessible.gov.

The contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

Section 508 of the Rehabilitation Act requires Federal agencies to make their electronic and information technology accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology.

All electronic and information technology (EIT) procured through this task order must meet the applicable accessibility standards specified in 36CFR1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this task order are listed below.

The standards define Electronic and Information Technology, in part, as "any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information." The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport and production. This includes computers, software, networks, peripherals, and other types of electronic office equipment.

APPLICABLE STANDARDS, WHICH APPLY TO THIS ACQUISITION

Section 1194.21: Software Applications and Operating Systems _____X____.

Section 1194.22: Web-based Internet Information and Applications _____X_____.

Section 1194.23: Telecommunications Products _____.

Section 1194.25: Self-Contained, Closed Products _____.

Section 1194.26: Desktop and Portable Computers _____.

Section 1194.31: Functional Performance Criteria _____.