

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. CONTRACT ID CODE	PAGE OF PAGES	
			J	1	31
2. AMENDMENT/MODIFICATION NO. 0003	3. EFFECTIVE DATE 20-Aug-2009	4. REQUISITION/PURCHASE REQ. NO. W45XJ38026N003		5. PROJECT NO.(If applicable)	
6. ISSUED BY USA MED RESEARCH ACQ ACTIVITY 820 CHANDLER ST FORT DETRICK MD 21702-5014	CODE W81XWH	7. ADMINISTERED BY (If other than item 6) USA MED RESEARCH ACQ ACTIVITY ATTN: WILLIAM DELISE 301-619-2480 BILL.DELISE@US.ARMY.MIL FORT DETRICK MD 21702		CODE	W81XWH
8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code)			X	9A. AMENDMENT OF SOLICITATION NO. W81XWH-09-R-0032	
			X	9B. DATED (SEE ITEM 11) 18-Aug-2009	
				10A. MOD. OF CONTRACT/ORDER NO.	
				10B. DATED (SEE ITEM 13)	
CODE			FACILITY CODE		
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS					
<input checked="" 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 checked="" 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).					
C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:					
D. OTHER (Specify type of modification and authority)					
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input type="checkbox"/> is required to sign this document and return _____ copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) TITLE: Video Network center (VNC) Services and Support for USAMITC The purpose of this Amendment is to correct discrepancies in the PWS and Labor Categories list and to note that the Statement: "THIS NOTICE IS PROVIDED FOR INFORMATION PURPOSES ONLY. THIS OPPORTUNITY IS AVAILABLE ONLY TO CONTRACTORS UNDER W81XWH09R0032" on FedBizOpps Announcements should NOT have been applied to this Solicitation. This Solicitation is a Section 8(a) Competitive and is NOT restricted to the incumbents. See attached Summary of Changes.					
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)		
			TEL:	EMAIL:	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA		16C. DATE SIGNED	
_____ (Signature of person authorized to sign)		BY _____ (Signature of Contracting Officer)		20-Aug-2009	

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION SF 1449 - CONTINUATION SHEET

NOTE: CHANGES INDICATED IN RED.

The following have been modified:

**EVALUATION CRITERIA
for Video Network Center (VNC) PWS**

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

This is a best value procurement. The Government may elect to award to other than the lowest cost, based on the evaluation of the non-cost factors and the best value to the Government. As individual factors, Technical Approach is the most important of the factors. Management Approach and Past Performance Approach rank second and third in importance, respectively. Cost and Price is the least important of all the factors. When considered together Technical Approach, Management Approach, and Past Performance are significantly more important than Cost and Price.

Technical Approach.

The Government will assess the degree to which the offeror's techniques, methods, and processes are likely to minimize risk and result in successful completion of the tasks in the PWS. The Government will assess the offeror's ability to produce contract deliverables by examining the degree to which the offeror's explanation of the manner and methods to be used are likely to result in the desired outcomes. The Government will assess the degree to which the offeror's technical proposal demonstrates experience in all areas of the PWS.

Management Approach.

The Government will assess the degree to which the offeror's management procedures and capabilities are likely to result in successful contract performance. The Government will assess the extent to which the labor categories proposed by the offeror are likely to successfully complete the tasks in the PWS. The Government will assess the offeror's understanding of the importance of all the positions by the number and quality of Commitment Resumes submitted for these positions, as well as an Employee Capture Plan. The Plan will be assessed as to the understanding of the need to retain contractor employees that possess corporate knowledge and expertise whenever possible. However, retaining contractor employees with corporate knowledge can never come at the expense of fiscal discipline, and that labor prices must be reasonable. The Government will assess the offeror's ability to comply with the PWS by reviewing the proposed staffing plan with regard to the appropriateness of proposed labor categories and the qualifications of personnel. The Government will assess the degree to which teaming agreements, when proposed, demonstrate capabilities necessary to complete the work contained in the PWS and exhibit efficient and effective teaming techniques. The Government will assess the offeror's ability to attract and retain skilled employees from a Recruitment and Retention Plan.

Past Performance Approach.

This evaluation factor will first assess the relevancy of each offeror's past performance. Past performance of the same size, scope, and complexity as the instant requirement will be deemed most relevant. Then, an assessment of the quality of each offeror's relevant past performance will be made. Qualitative information can be gathered through the use of databases, questionnaires, reference checks, and/or personal knowledge. In determining an overall rating for this factor, consideration will also be given to the number and severity of problems encountered by

each offeror in their documented past performances and the demonstrated effectiveness of corrective actions taken. The overall rating will focus on over-all results, not simply problem-free management.

Offerors should submit at least 3 recent (within the past 5 years) past performance examples. The Army reserves the right to consider other past performance information at its disposal. If any offeror is truly a new entity and none of the company principals have relevant work experience, the offeror will be considered to have no past performance. In the event an established offeror is simply without a record of past performance, the offeror's lack of past performance will be evaluated as an unknown risk having no favorable or unfavorable impact on the evaluation.

Cost and Price Evaluation.

The degree to which the offeror's proposed rates represent a fair and reasonable price will be evaluated using the techniques in FAR 15.305(1), which provides that comparison of the proposed prices will usually satisfy the requirement for price analysis. Offerors shall provide a spreadsheet listing all labor categories, hourly rates and extended labor costs. **Provide cost for the initial period of performance and the option year (pricing will be for 2 years).** Provide prices that both evaluate the reasonableness and the cost realism of the proposed cost/prices. The price evaluation will be inclusive of all option prices.

Relative Order of Importance of Evaluation Factors:

This is a best value procurement. The Government may elect to award to other than the lowest price, based on the evaluation of the non-cost factors and the best value to the Government.

As individual Evaluation Factors, Technical Approach is the most important factor. Management Approach and Past Performance Approach rank second and third in importance, respectively. When technical, past performance, and management factors are considered together, they are significantly more important than cost or price. Cost and Price is determined to be less significant than any of the factors. If two or more proposals are evaluated as relatively equal in technical merit (non-cost factors), cost and price could become the deciding factor in awardee selection.

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

ADDITIONAL INSTRUCTIONS FOR SUBMISSION OF OFFERS

1. COMMUNICATIONS REGARDING THIS SOLICITATION

TELEPHONIC REQUESTS FOR INFORMATION REGARDING THIS SOLICITATION WILL NOT BE HONORED.

All questions MUST be submitted in writing via email NO LATER THAN BY 3:00 PM Eastern Daylight Time, Thursday, 27 August 2009. Questions must be sent via EMAIL to bill.delise@us.army.mil SUBJECT: W81XWH-09-R-0032, Video Network Center for USAMITC. File attachments should be no larger than 2MB.

Answers to questions will be addressed via an amendment to the solicitation which will be posted on the USAMRAA and Army Single Face to Industry web sites as soon as possible after the deadline for questions has closed. In the event multiple questions address the same issue, the Government reserves the right to answer a representative question that best exemplifies the issue.

2. Proposal submission requirements: In order to be considered for possible contract award, the Offeror shall submit their proposals electronically via Army Single face to Industry. DUPLICATE COPIES WILL NOT BE SENT VIA E-MAIL. Proposals shall be submitted as follows:

- a. Technical Proposal
- b. Management Proposal
- c. Past Performance Approach
- d. Separate Cost and Price Proposal (to include business aspects-cover letter, signed amendments, signed certifications, etc.)

Each (a thru d) shall be submitted as a separate volume.

Font size shall be 12pt and margins must be at least one inch. See proposal page limitations, information on copies and volume assembly below.

A. TECHNICAL PROPOSAL - The offeror shall submit a Technical Proposal addressing the following:

TECHNICAL APPROACH.

The offeror shall describe the techniques, methods, and processes it plans to use to minimize risk and accomplish the tasks specified in the PWS. The offeror shall address the manner and method of the planned execution of the required deliverables. The offeror shall discuss its technical expertise to cover all aspects of the PWS with emphasis on providing Video Network Center (VNC) Operations. Clarity, completeness and conciseness are essential, and the quality of the proposal should be representative of the offeror's product.

The page limitation for Technical Approach is 30 pages. Pages in excess of the limitation will not be considered.

B. MANAGEMENT PROPOSAL – The offeror shall submit a Management Proposal addressing the following:

MANAGEMENT APPROACH.

The offeror shall describe management procedures and capabilities that will be used to ensure successful contract performance. The offeror shall provide proposed labor categories and descriptions to perform the work described in the PWS. The offeror shall provide Commitment Letters and Resumes for qualified candidates. Resumes shall demonstrate the education and experience necessary to complete the tasks in the PWS. The offeror shall provide an Employee Capture Plan that address the efforts to retain contractor employees who have knowledge and expertise required. The offeror shall provide a staffing plan that addresses the accomplishment of the PWS with regard to assigned personnel, emphasizing the qualifications of personnel. Offerors shall describe the ability to attract and retain skilled employees with a Recruitment and Retention Plan. Offerors shall describe planned teaming

arrangements. Specifically, offerors shall detail how the team will function and how the team will interact with and relate to the Government.

The page limitation for Management Approach is 25 pages. Pages in excess of the limitation will not be considered.

C. PAST PERFORMANCE APPROACH – The offeror shall submit Past Performance Approach as follows:

PAST PERFORMANCE APPROACH.

The proposal shall clearly demonstrate past performance that is relevant to the RFP's PWS. This includes, but is not limited to, the offeror's record of 1) meeting milestones; 2) timely submission of deliverables; and 3) technical competency. The offeror's proposal must include at least three relevant past/current performance examples within the last five years. If the offeror has been in business less than three years, previous relevant experience from the offeror's principals or key personnel may be provided. The information shall contain the following:

Project or Contract Title

Contract Number, contracting agency, type of contract and total contract dollars

Date of contract and period of performance

Firm or Government agency for which work was performed

Point of Contact (Contracting Officer or Contracting Officer's Representative). Name, title, address, and telephone number

Brief description of how the cited work is the same as the proposed effort.

Offerors that propose to use subcontractors (or teaming arrangements) to perform major or critical aspects of this requirement must provide the above information on each of the subcontractors or team members.

Offerors shall have past/current customers complete the Past Performance Questionnaire. Past/current customers must submit the questionnaire directly to bill.delise@us.army.mil prior to the closing of the solicitation.

There is no page limitation for Past Performance Approach.

D. COST AND PRICE PROPOSAL – The offeror submit cost and price information as follows:

COST AND PRICE PROPOSAL.

The offeror shall submit proposed rates. Offerors shall provide a spreadsheet listing all labor categories, hourly rates and extended labor costs. Provide cost for the initial period of performance and the option year. Provide prices that both address the reasonableness and the cost realism of the proposed cost/prices. Information submitted shall be inclusive of all option prices.

There is no proposal page limitation for Price and Cost Proposal.

LABOR CATEGORIES**1 FTE = 1,920 HOURS**

Labor Category	MINIMUM	MAXIMUM	Minimum Hours	Hourly Rate	Minimum Total Cost
Operations Manager	0	1	0		
Administrative Assistant	1	1	1920		
Scheduler (Level I)	4	22	7680		
Scheduler (Level II)	0	8	0		
Bridge Operator (Level I)	1	10	3840		
Bridge Operator (Level II)	0	3	0		
Technical Support Technician (Level I)	1	10	1920		
Technical Support Technician (Level II)	0	3	0		
IP Video Network Engineer (Level I)	2	5	3840		
IP Video Network Engineer (Level II)	0	5	0		
Wide Area Network Engineer (Level III)	0	2	0		
Database Programmer/Metrics	0	1	0		
Technical Writer	0	1	0		
Videoconferencing Facilitator	0	8	0		

*NON-LABOR/ODCs

\$50,000.00(EST)

*Government furnished estimate

PERFORMANCE WORK STATEMENT (PWS)

United States Army Medical Information Technology Center (USAMITC)

Customer Support Division

Video Network Center (VNC)

1. Introduction

At USAMITC, we design, develop, deploy, and sustain Information Management / Information Technology (IM/IT) systems. Our product management professionals and IM/IT engineers have extensive experience to cover the life cycle of IM/IT capabilities, and we research, evaluate, and integrate leading-edge technology to help our customers solve their IM/IT challenges.

Background

USAMITC has been chartered to maintain and support videoconferencing systems throughout the AMEDD and Tri-Service. This includes all Army, Navy, Air Force, Coast Guard, Veterans Administration, and public Hospitals other Medical Treatment Facilities and can include videoconferencing support, cabling support, hardware and software purchase and maintenance as well as any other service and/or support that can be provided to the various services.

Video Systems Development, Deployment, and Sustainment

Our center performs all tasks to accomplish successful video teleconferencing, scheduling conferences, performing live video call monitoring. We provide project support for the AMEDD for all aspects of video teleconferencing to include :

- Scheduling of video and audio conferences
- Project Development and Coordination
- Live conference monitoring
- Video Teleconferencing (VTC) Requirements Analysis
- Hardware engineering and installations
- Enterprise VTC network monitoring and engineering

To ensure new video capabilities are ready to be deployed, VNC provides an independent testing/assessment environment. Quality assurance services include security testing, Technical Support testing and evaluation, system pilots, and system documentation. Once deployed, USAMITC provides software support through sustainment services such as upgrades and modifications, application maintenance, and technical customer support.

2. Objective

To obtain the following services and skills: Tier I support for live audio and video conferences. Scheduling and coordination of audio and video conferences. Tier I and II support for troubleshooting and designing of video conferencing systems and rooms. Tier I and II engineering, installation and operational support of the existing and planned IP Video infrastructure.

3. Tasks to be performed

The main tasks the Contractor will be required to perform are as follows:

(Specific tasks will be specified in each Task Order, as well as a Quality Assurance Surveillance Plan),

A. Operations Manager

- Assist in managing in daily operations of the VNC overseeing the planning, directing, and coordinating the

operations to identify work activities to be accomplished and scheduled according priorities.

- Assist in Monitoring team activity and evaluate workload.
- Assist in prepare work schedules and assign specific duties.
- Assist in planning, directing, or coordinating the operations to include the determining the most effective use of materials and human resources.
- Assist in handling correspondence and customer questions, concerns and complaints.
- Assist in directing and coordinating activities of each section concerned with Scheduling, Bridge Operations and Technical/Project Support
- Assist in directing Project Support activities in relation to development, design and implementation of supported projects.
- Assist in tracking operational funding and daily activity reports.
- Assist in conducting general management and administration services.
- Assist in establishing and implementing departmental policies, goals, objectives, and procedures, conferring with technical leads and other staff members as necessary and ensuring compliance
- Assist in performing customer service work such as greeting and assisting customers as well as in-house briefings and demonstrations of capabilities for walkthrough customers.
- Assist in coordinating, planning and directing activities with marketing and other departments as required.

B. Administrative Assistant

- Provide first line customer support for videoconferencing operations.
- Answer and direct all incoming calls to appropriate Video Network Center personnel.
- Manage and schedule MITC videoconferencing rooms determining resource availability and ensuring that Information Engineer is notified of discrepancies and room participation in multipoint videoconference.
- Ensure that MITC videoconference rooms are open and operational, daily.
- Perform as backup for the schedulers.
- Handles multipoint video and audio conferencing requests.
- Responsible for determining resource availability for accommodation of each conference that requires the tracking of multiple conference variables including MCU port availability, approximate bandwidth availability, date availability, time zone differences and other incidents as they occur.
- ARIMS (Army Records Information Management System) for Division
- Assist with completing required documentation for logistics and procurement.
- Conduct audit of any submitted documentation to ensure that requirements are being met
- Assist in Coordinating maintenance schedules with vendors and/or manufacturers contracted to provide the these services.

C. VNC Scheduler (Level I)

- Provide first line customer support for video and audio teleconferencing operations.
- Processes all multipoint video and audio conferencing requests.
- Responsible for determining resource availability for accommodation of each conference.
- Tracking of multiple conference variables including MCU and audio bridge port availability.
- Manage bandwidth availability, date availability, time zone differences, and other limiting variables.
- Coordinate video conference room scheduling conflicts with multiple remote room facilitators.
- Coordinate with bridge operations for all last minute changes to scheduled conferences.
- Schedule and coordinate with other video and audio bridging operations within the Department of Defense and other government agencies.

Suggested Qualifications

- 1-3 years experience in working as a video and audio conferencing scheduling agent

D. VNC Scheduler (Level II, Technical Lead)

- Technical Lead for all operations encompassing Scheduling operations
- Provide first line customer support for video and audio teleconferencing operations.
- Processes all multipoint video and audio conferencing requests.

- Responsible for determining resource availability for accommodation of each conference.
- Tracking of multiple conference variables including MCU and audio bridge port availability.
- Manage bandwidth availability, date availability, time zone differences, and other limiting variables.
- Coordinate video conference room scheduling conflicts with multiple remote room facilitators.
- Coordinate with bridge operations for all last minute changes to scheduled conferences.
- Schedule and coordinate with other video and audio bridging operations within the Department of Defense and other government agencies.

Suggested Qualifications

- Must demonstrate considerable initiative and skill in developing and participating in a team environment
- 3-5 years direct experience as (or performing related duties of) the Technical Lead for Scheduling Operations required

E. VNC Bridge Operator (Level I)

- Provide technical expertise in videoconferencing equipment and technology to ensure successful multipoint videoconferencing across a Multipoint Conferencing Unit (MCU).
- Provide Tier I troubleshooting support for all active bridge operations.
- Monitor video and audio conferences to assure proper operation of all endpoint and transmission facilities.
- Perform video and audio requests by conference participants to add, drop, mute, or change, endpoints during active calls.
- Monitor requests of conference participants to extend conferences when requested.
- Conducts video and audio checks on all conferences during setup of conferences.
- Perform video site certifications for all video endpoints and other government video bridging centers.
- Responsible for system administration responsibilities of all enterprise VNC systems.
- Application administrator for all enterprise VNC systems
- Responsible for compliance of all IA security requirements for VNC operations.
- Responsible for coordination and troubleshooting with WAN/LAN service providers.
- Responsible for accuracy of active customer database used by VNC.

Suggested Qualifications

- 3-5 years direct work experience working in Bridge Operations required

F. VNC Bridge Operator (Level II, Technical Lead)

- Technical Lead for all operations encompassing Bridge Operations
- Provide technical expertise in videoconferencing equipment and technology to ensure successful multipoint videoconferencing across a Multipoint Conferencing Unit (MCU).
- Provide Tier I troubleshooting support for all active bridge operations.
- Monitor video and audio conferences to assure proper operation of all endpoint and transmission facilities.
- Perform video and audio requests by conference participants to add, drop, mute, or change, endpoints during active calls.
- Monitor requests of conference participants to extend conferences when requested.
- Conducts video and audio checks on all conferences during setup of conferences.
- Perform video site certifications for all video endpoints and other government video bridging centers.
- Responsible for system administration responsibilities of all enterprise VNC systems.
- Application administrator for all enterprise VNC systems
- Responsible for compliance of all IA security requirements for VNC operations.
- Responsible for coordination and troubleshooting with WAN/LAN service providers.
- Responsible for accuracy of active customer database used by VNC.

Suggested Qualifications

- 3-5 years direct experience as (or performing related duties of) the Technical Lead for Bridge Operations required

G. VNC Technical Support Technician (Level I)

- Performs Tier I & II customer support functions to include installation, maintenance, design and troubleshooting for all types of videoconferencing equipment.
- Load and configure videoconferencing software applications either onsite or by remotely directing the customer.
- Integrate complex videoconference equipment with peripherals and other video and audio devices.
- Perform preventive maintenance on video and audio hardware.
- Responsible for determining the impact of new software updates on existing hardware and overall network operation. Conducts extensive testing of software releases.
- Troubleshoots network anomalies, conducts test and evaluations to ensure optimum network operation.
- Performs site surveys in support of customer's acquisition of new videoconferencing equipment and/or room design features.
- Engineer hardware and software solutions in support of customer's acquisition of new videoconferencing equipment and/or room design features
- Conducts remote and onsite videoconferencing training for room facilitators, conference participants and equipment users.
- Responsible for Tier II and III troubleshooting with WAN/LAN service providers.

Suggested Qualifications

- 3-5 years experience in working Technical and Project support for videoconferencing

H. VNC Technical Support Technician (Level II, Technical Lead)

- Technical Lead for all operations encompassing Technical and Project Support
- Performs Tier I & II customer support functions to include installation, maintenance, design and troubleshooting for all types of videoconferencing equipment.
- Load and configure videoconferencing software applications either onsite or by remotely directing the customer.
- Integrate complex videoconference equipment with peripherals and other video and audio devices.
- Perform preventive maintenance on video and audio hardware.
- Responsible for determining the impact of new software updates on existing hardware and overall network operation. Conducts extensive testing of software releases.
- Troubleshoots network anomalies, conducts test and evaluations to ensure optimum network operation.
- Performs site surveys in support of customer's acquisition of new videoconferencing equipment and/or room design features.
- Engineer hardware and software solutions in support of customer's acquisition of new videoconferencing equipment and/or room design features
- Conducts remote and onsite videoconferencing training for room facilitators, conference participants and equipment users.
- Responsible for Tier II and III troubleshooting with WAN/LAN service providers.

Suggested Qualifications

- 3-5 years direct experience as (or performing related duties of) the Technical Lead for Technical and Project Support required

I. VNC IP Video Network Engineer (Level I)

- Responsible for the designing, planning, managing and implementation of IP Video LAN installations in Medical Treatment Facilities (MTF)
- Provide Network infrastructure support for IP Video.
- Troubleshoots network anomalies, conducts test and evaluations to ensure optimum network operation.
- Performs site surveys in support of customer's new videoconferencing equipment and/or systems.
- Responsible for integration of new hardware securely into existing MTF networks, including LAN, WAN, VPN, VLANs, and other hardware and software configured networks in compliance with network security requirements of the AMEDD.

- Responsible for troubleshooting, maintaining, and understanding the technical areas of WAN and LAN, communications and infrastructure equipment, such as intrusion detection systems, firewalls, proxies, broader controllers, gateways, gatekeepers, VPNs and other networking hardware.
- Performs Tier I & II customer support functions to include installation, maintenance, design and troubleshooting for all types of videoconferencing equipment.
- Load and configure videoconferencing software applications either onsite or by remotely directing the customer.
- Integrate complex videoconference equipment with peripherals and other video and audio devices.
- Perform preventive maintenance on video and audio hardware.
- Conducts extensive testing of software releases to determining the impact of new software updates on existing hardware and overall network operation.
- Performs site surveys in support of customer's acquisition of new videoconferencing equipment and/or room design features.
- Engineer hardware and software solutions in support of customer's acquisition of new videoconferencing equipment and/or room design features
- Conducts remote and onsite videoconferencing training for room facilitators, conference participants and equipment users.
- Responsible for Tier II and III troubleshooting with WAN/LAN service providers.

Suggested Qualifications

- 3-5 years direct experience as an IP Video Network Engineer and associated disciplines required

J. VNC IP Video Network Engineer (Level II)

- Assist in the designing, planning, managing and implementation of IP Video LAN installations in Medical Treatment Facilities (MTF)
- Provide Network infrastructure support for IP Video.
- Troubleshoots network anomalies, conducts test and evaluations to ensure optimum network operation.
- Performs site surveys in support of customer's new videoconferencing equipment and/or systems.
- Performs integration of new hardware securely into existing MTF networks, including LAN, WAN, VPN, VLANs, and other hardware and software configured networks in compliance with network security requirements of the AMEDD and DoD.
- Performs troubleshooting, maintaining, and understanding the technical areas of WAN and LAN, communications and infrastructure equipment, such as intrusion detection systems, firewalls, proxies, broader controllers, gateways, gatekeepers, VPNs and other IPV networking hardware.
- Performs Tier I & II customer support functions to include installation, maintenance, design and troubleshooting for all types of videoconferencing equipment.
- Load and configure videoconferencing software applications either onsite or by remotely directing the customer.
- Integrate complex videoconference equipment with peripherals and other video and audio devices.
- Perform preventive maintenance on video and audio hardware.
- Conducts extensive testing of software releases, determining the impact of new software updates on existing hardware and overall network operation.
- Performs site surveys in support of customer's acquisition of new videoconferencing equipment and/or room design features.
- Engineer hardware and software solutions in support of customer's acquisition of new videoconferencing equipment and/or room design features
- Conducts remote and onsite videoconferencing training for room facilitators, conference participants and equipment users.
- Responsible for Tier II and III troubleshooting with WAN/LAN service providers.

Suggested Qualifications

- 5-7 years direct experience as an IP Video Network Engineer and associated disciplines required

K. VNC Wide Area Network Engineer (Level III)

- Provide Network infrastructure support for IP Video.
- Troubleshoots network anomalies, conducts test and evaluations to ensure optimum network operation.
- Provides network traffic status and suggested network changes to support enterprise video traffic load.
- Coordinates directly with DVS, DISA, DSN, and other WAN providers to trouble shoot and restore circuits and systems.
- Performs all circuit activation processes with TIMPO, DISA, commercial ISPs and telephone providers and other agencies
- Performs integration of new hardware into existing MTF networks, including LAN, WAN, VPN, VLANs, and other hardware and software configured networks in compliance with network security requirements of the AMEDD.
- Performs troubleshooting, maintaining, and understanding the technical areas of the WAN, communications and infrastructure equipment, such as circuits, firewalls, gateways, VPNs and other networking hardware.
- Performs Tier III customer support functions to include installation, maintenance, design and troubleshooting for all types of videoconferencing equipment.
- Load and configure videoconferencing software applications either onsite or by remotely directing the customer.
- Perform preventive maintenance on WAN hardware.
- Conducts extensive testing of software releases determining the impact of new software updates on existing hardware and overall network operation. Performs site surveys in support of customer's acquisition of new videoconferencing equipment and/or room design features.
- Engineer hardware and software solutions in support of customer's acquisition of new videoconferencing equipment and/or room design features
- Conducts remote and onsite videoconferencing training for room facilitators, conference participants and equipment users.
- Responsible for Tier III troubleshooting with WAN/LAN service providers.

Suggested Qualifications

- 5-7 years direct experience as an Wide Area Network Engineer and associated disciplines required

L. Database Programmer/Metrics

- Assist to, designs, implements and maintains current Microsoft SQL and Paradox databases
- Assist with design, creation, and maintenance of computerized databases.
- Assist with the quality control and auditing of databases to ensure accurate and appropriate use of data.
- Assists management to develop database strategies to support organization requirements.
- Consults with and advises users on access to various databases.
- Works directly with users to resolve data conflicts and inappropriate data usage.
- Assist with maintenance of database dictionaries, overall monitoring of standards and procedures, and integration of systems through database design.
- Enters and maintains data dictionary information, data keyword lists, and dictionary forms.
- Reviews all information to be entered into the dictionary to assure adherence to standards and to ensure that all requirements are met.
- Maintains current library of each processing system's information recorded in the dictionary.

Suggested Qualifications

- Must have an in depth knowledge of Crystal Reports design and development to create customized metric reports using existing databases.
- Must be able to troubleshoot existing reporting issues.
- Demonstrate competence to work at levels of database management.

M. Technical Writer

- Assist in preparing and/or maintaining systems, programming, and operational documentation, procedures,

and methods including user manuals and reference manuals.

- Maintains a current internal documentation library.
- Provides or coordinates special documentation services as required.
- Ensures that documents follow the style laid out in the organization's style guide.
- Assists in maintaining the style guide.
- Suggests revisions to the style guide as appropriate.
- Maintain all standards for formatting and report writing as defined by all U.S.Army and Department of Defense (DoD) policies and procedures.

N. Videoconferencing Facilitator (On and Off-site)

- Evaluate customer's video and audio conferencing needs and expectations in order to coordinate scheduling effort.
- Acts as the central contact person who is responsible for scheduling and organizing point to point and multipoint audio and videoconferences conferences.
- Ensures that the videoconference rooms are reserved at each participating site (factor in time for equipment setup, testing, and takedown if needed)
- Ensure that remote site facilitators are aware of Customer expectations of them before, during and after the videoconference to include any special equipment or room configuration need.
- Conduct periodic test calls.
- Prepare agenda with program date and time to all participants.
- Provide an overview of the videoconferencing mode selected for the meeting.
- Provide an overview of the microphone mode selected for the meeting and instruct participants on interaction using the microphones.
- Track and manage utilization of video conferencing rooms.
- Conduct support for videoconferencing equipment and peripheral devices.
- Contact local or enterprise videoconferencing technical support staff should technical issues arise.
- Assist technical point of contacts if necessary.
- Report any equipment issues to maintenance provider/s when necessary.

4. PlanView.

Contract personnel shall utilize PlanView. The Government will furnish licenses and training. Contract personnel may perform one or all of the following tasks: collect time, input time and close work. The Government will schedule an initial meeting with contractor personnel to discuss the roles of contract personnel, and the goals and objectives of this requirement.

5. Personnel Requirements

The historical level of effort for this statement of work is outlined below and based on 1920 hours per year for each category:

Labor Category	Minimum	Maximun
Operations Manager	0	1
Administrative Assistant	1	1
Scheduler (Level I)	4	22
Scheduler (Level II)	0	8
Bridge Operator (Level I)	1	10
Bridge Operator (Level II)	0	3
Technical Support Technician (Level I)	1	10
Technical Support Technician (Level II)	0	3
IP Video Network Engineer (Level I)	0	5
IP Video Network Engineer (Level II)	0	5

Wide Area Network Engineer (Level III)	0	2
Database Programmer/Metrics	0	1
Technical Writer	0	1
Videoconferencing Facilitator	0	8

6. Duty Location

The contractor's personnel will primarily be required to support USAMITC in Bldg 3272

Howitzer Street, Fort Sam Houston, Texas 78234-5087.

The duty location will be specified in each task order.

7. Period of Performance.

Performance of this PWS will commence on contract award for 12 months, plus 1 options year.

8. Hours of Operation.

Work will normally be performed during regular duty hours, Monday-Friday, excluding federal holidays, eight hours per day during the period 0500 to 1700 with one hour for lunch. During the period of performance of this contract the VNC mission maybe expanded to cover a global video mission. The hours of operation maybe expanded up to 24 hour coverage of the mission. A tour of duty shall be established with the Task Manager (TM) and the Contracting Officer Representative (COR) upon contract award. Total hours worked shall not exceed the number of hours ordered in the schedule. Subject to prior approval, variation in work schedule is acceptable when the total contract hours are not exceeded and no obligation is incurred requiring contractor personnel to be paid overtime. If overtime is required, it will be worked ONLY with approval from the TM or COR.

9. Extended Work Week (EWW):

If required, contractor must provide contract staff if the EWW is necessary. A EWW may be required if contractor is requested to man the Videoconferencing Center outside the normal scheduled duty hours. The videoconferencing staff consists of schedulers, bridge technicians and support technicians.

10. Delivery Schedule.

The following table contains contract.

Deliverable	Due Date
Invoice to include, personnel labor hours, and current and cumulative expenditures.	NLT the 15 th of the following month.

11. Invoicing

The contractor shall submit invoicing through Wide Area Work Flow (WAWF) and forward an information copy to the COR containing invoice accumulated data. Charges will be based on labor for the preceding month NLT fifteen (15) work days into the following month. Billing will be monthly in arrears and will include the Total Hours Worked (separating regular and overtime hours); and the Total Loaded Labor Rate for Each Reporting Period. The Invoice will also include the total number of hours used by each labor category; a cumulative total for each labor category; a total for all labor categories and a cumulative total for all labor categories. The Task Manager shall verify that the hours are correct while utilizing Government records to verify the hours worked. ODC charges will be listed on the monthly invoice as a separate charge. Backup documentation must be submitted with the copy of the invoice to the COR as well as with the original invoice.

12. Security

Contractor personnel must be able to obtain a Satisfactory NAC/LC, ADP Level II access. There is no requirement

for or access to classified material.

a.. **The Common Access Card (CAC).**

The CAC will be issued to eligible DoD contractor personnel. Assistance in obtaining the CAC will be provided by the COR.

b. **Security Environment.**

Contract personnel will be working in a restricted, secured environment and shall be responsible for compliance with Army Physical Security Program AR 190-13. This regulation is located in the USAMITC Security Office

c. **Security In-Briefing.**

Prior to reporting to the work site, contractor personnel shall report to the USAMITC Security Office for issuance of a government badge and security briefing. Contract personnel shall be required to undergo a National Agency Check (NAC) security investigation. If derogatory information is reported, the Commander will determine whether it is in the interests of national security to continue the contractor's status. If contract employee is replaced by another contract employee at no fault/request of the Government, the contractor shall be responsible for costs of replacement employee's NAC investigation.

d. **Security Badges.**

Personnel shall wear an identifying badge issued by the Government at the site. The badge shall be worn on outer clothing between the neck and waist on the front part of the body and be visible at all times.

13.0 OTHER TERMS, CONDITIONS, AND PROVISIONS

13.1 Agreements

13.1.1 Authorized Use Policy Agreement

The Contractor shall ensure that the Authorized Use Policy (AUP) Agreement (Appendix A) is signed by all staff assigned to, including all subcontractors and consultants, or performing on this Task order and adhere to the terms of that AUP. Assignment of staff who has not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor.

13.1.2 Privileged Access Agreement

The Contractor shall ensure that the Privileged Access Agreement (PAA) (Appendix B) is signed by all staff with privileged access to information systems that are assigned to, including all subcontractors and consultants, or performing on this Task order and adhere to the terms of that privileged access statement, protecting the information and information systems of the Government. Assignment of staff who has not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor.

13.1.3 Certificate of Non Disclosure

The Contractor shall ensure that the Certificate of Non-Disclosure (Appendix C) is signed by all staff assigned to, including all subcontractors and consultants, or performing on this Task order and adhere to the terms of that non-disclosure statement, protecting the procurement sensitive information of the Government and the proprietary information of other contractors. Assignment of staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor.

13.2 Information Assurance

13.2.1 General Security Requirements

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of government data. As a minimum, this

shall include provisions for personnel security, electronic security and physical security as listed in the sections that follow:

13.2.1.1 Personnel Security

- a. The contractor shall comply with DoD Directive 8500.1, "Information Assurance (IA)," DoD Instruction 8500.2, "Information Assurance (IA) Implementation," DoD Directive 5400.11, "DoD Privacy Program," DoD 6025.18-R, "DoD Health Information Privacy Regulation," and DoD 5200.2-R, "Personnel Security Program Requirements."
- b. Contractor responsibilities for ensuring personnel security include meeting the following requirements:
- Follow the USAMITC Security Office guidelines for submittal of Information Technology (IT) background investigations and security clearances and ensure all contractor personnel are designated as IT-I, IT-II, or IT-III where their duties meet the criteria of the position sensitivity designations. Contact the USAMITC IA Office for guidance on the appropriate IT levels for personnel on the contract.
 - Initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to Sensitive Information (SI).
 - Immediately report to the USAMITC Security Office and deny access to any automated IS (AIS), network, or SI information if a contractor employee filling a sensitive position receives an unfavorable adjudication, if information that would result in an unfavorable adjudication becomes available, or if directed to do so by the appropriate government representative for security reasons.
 - Ensure that all contractor personnel receive information assurance (IA) training before being granted access to ISS, networks, and/or SI information.

13.2.1.2 Security and Privacy. The Contractor shall –

- a. Provide physical security for all material, equipment, data, and information handled during contract performance, in accordance with AR 190-13, The Army Physical Security Program, AR 190-51, Security of Unclassified Army Property (Sensitive and Nonsensitive), and command policies, procedures, and regulations.
- b. Obtain background investigations for all personnel assigned to this contract. Each task order will specify appropriate IT levels and security clearance requirements, in accordance with the provided DD Form 254, for the tasks performed. Work performance that requires access to classified communications security (COMSEC) information will require a final security clearance at the requisite level. The required security clearances and SCI access indoctrination, as specified, shall be in force or submitted with no issues that would prevent the issuance of an interim clearance for all assigned personnel at task order start date. Individuals who have been barred or were previously barred from the installation pursuant to Title 18 U.S.C. Section 1382 shall not be allowed to enter or work on the installation.
- The Contractor shall be required to gain access to the USAMITC network for performance of this task and shall follow all guidelines and policies established for the use of this network. As such, contractor personnel shall undergo appropriate background investigation and security awareness training. The Contractor shall be prepared for this process to take at least two (2) weeks, if not longer. The Contractor shall submit the appropriate forms for background investigation commiserate to the IT-level and/or security clearance identified in the task order to the Office of Personnel Management and obtain receipt confirmation.
 - Contractors must notify the USAMITC Security Office when the Contractor's security officer has submitted the SF85P user form to OPM for new employees. Upon termination of a contractor employee from the USAMITC Contract, contracting companies must notify the USAMITC Security Office and OPM of the action, including the termination date.
 - Contactor must obtain a DoD Common Access Card (CAC) prior to receiving access to the USAMITC Network. Contactor shall contact the USAMITC Security Office for guidance on obtaining a DoD CAC at

(210) 295-3331. Upon termination of the period of performance, all Government issued access cards will be turned in to the COR.

13.2.1.3 Access to Protected Information. If, during the performance of this procurement, Contractor personnel obtain access, by any means, to protected information, including trade secrets or proprietary information of other contractors, Government source selection information, HIPAA, Privacy Act information, or any other information with distribution limited by the Government, Contractor personnel shall in no way divulge any such information except as it relates to the performance of this procurement within USAMITC itself, or shall not otherwise use or disclose this information for their personal gain, the gain of their employer, or the gain of anyone else. Contractor personnel shall notify the Contracting Officer, their Task Manager, or the Contracting Officer Representative of any potential organizational conflict of interest created by any such access. A nondisclosure agreement, however, will not overcome an Organizational Conflict of Interest (OCI) as defined in FAR part 9.5. Moreover, compliance with the Trade Secrets Act requires the consent of the owner of the proprietary information before another non-federal entity may be allowed access to such information. Accordingly, all Government Contractors are required to mark their proprietary information; any time the Contractor is given access to such marked information, it is incumbent upon the Contractor to inform the Contracting Officer of the access. Contractor personnel ordinarily will be required to sign a nondisclosure agreement before starting work under the contract. Failure to comply with this clause shall be deemed adequate cause for the removal of a Contractor employee from employment with the Contractor. The Contractor's employment contracts with its employees shall include a provision to provide for their removal under these conditions.

13.2.1.4 Health Insurance Portability and Accountability Act (HIPAA)

The contractor shall comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) requirements, specifically the administrative simplification provisions of the law and the associated rules and regulations published by the Secretary, Health and Human Services (HHS) and the published MEDCOM implementation directions. This includes the Standards for Electronic Transactions, the Standards for Privacy of Individually Identifiable Health Information and the Security Standards. It is expected that the contractor shall comply with all HIPAA-related rules and regulations as they are published and as USAMITC requirements are defined (including identifiers for providers, employers, health plans, and individuals, and standards for claims attachment transactions).

13.2.1.5 Dissemination of Information/Publishing

There shall be no dissemination or publication, except within and between the Contractor and any subcontractors or specified Integrated Product/Process Team (IPT) members who have a need to know, of information developed under this order or contained in the reports to be furnished pursuant to this order without prior written approval of the USAMITC TM or the Contracting Officer. USAMITC approval for publication will require provisions which protect the intellectual property and patent rights of both USAMITC and the Contractor.

13.3 Training & Certification.

13.3.1 The Contractor shall –

- a.** Provide required initial, supplemental, refresher, upgrade, and proficiency training for its personnel to maintain pace with technological advances. This training shall be at no additional cost to the Government.
- b.** Provide a minimum of eight hours of formal introductory ITIL training to its personnel within 90 days of assignment to USAMITC task orders. The instructor shall be certified in ITIL Foundations and use a course syllabus approved by the ITIL technical point of contact (TPOC) and COR.
- c.** Maintain a record of required training and IT certifications for its personnel and make them available for review upon COR or TM request .
- d.** Contractor personnel shall be appropriately certified prior to being engaged. At a minimum, contractor personnel must meet required DoD Approved Baseline Certifications as described in the DoD 8570.01-M,

“Information Assurance Workforce Improvement Program”, and Army BBP 05-PR-M-0002, “Information Assurance (IA) Training and Certification v2.0”, Table 1, for the IA Workforce level and category so designated in this PWS or on a task order.

e. In addition to the DoD Baseline IA certification requirement for their level, IAT level individuals (IAT-I/II/III) must also be certified in their computing environment (CE). IATs with privileged access **MUST OBTAIN APPROPRIATE COMPUTING ENVIRONMENT (CE) CERTIFICATIONS** for the components, devices and/or operating system(s) they support as required by USAMITC. The specific CE certification will be provided within this PWS and/or the task order (**See APPENDIX D**).

13.3.2 The Government will fund additional training at its discretion to meet task order requirements involving new or unique applications, tools, or processes.

13.3.3 Contractor personnel who perform systems administrator/network manager functions under this contract shall complete environment specific requisite training per DoD, Army and MEDCOM regulations and directives within six months of appointment. The Government-sponsored Systems Administrator/Network Manager (SA/NM) Security Course is available at Fort Huachuca, Arizona; Fort Gordon, Georgia; and accredited mirror training sites. Course substitution requires prior Army Chief Information Officer/G-6 approval. The Contractor shall submit any requests for course substitution to the COR.

14. Government Furnished

14.1 Facilities, Supplies, and Services.

The Government will provide workspace, working supplies, furniture, desktop computers, and access to business telephones (for business purposes only) and other equipment as needed to perform the tasks specified in this PWS. The government will provide any Government regulations and technical manuals needed.

14.2 Equipment.

Contractor personnel shall be responsible for all equipment issued to them and shall prudently maintain and guard equipment in accordance with proper office procedures. Government equipment may only be used in the performance of the tasks specified in this PWS. Equipment shall not leave the building without prior approval of the TM and issue of a DA Form 2062 from the hand receipt manager. Contractor personnel shall not modify or load software on computer equipment without prior approval by the Government.

15. Travel.

15.1 The Contractor shall provide support at CONUS and OCONUS locations to meet mission requirements. The TM with coordination with the COR will pre-approve all reimbursable travel. The Contractor shall obtain all necessary travel documentation to execute travel as required. The Contractor shall provide passports and visas for OCONUS travel for identified personnel. The Contractor shall ensure all Contractor employees comply with all guidance, instructions, and general orders applicable to U.S. Armed Forces and DOD civilians and issued by the Theater Commander or his/her representative. This will include any and all guidance and instructions issued based on the need to ensure mission accomplishment, force protection, and safety. The Contractor shall adhere to the following additional requirements when traveling to OCONUS locations:

15.2 Travel to Germany.

All persons who stay in Germany for more than 90 consecutive days are required to obtain a residence permit. US citizens in possession of a valid US passport do not need a visa for airport transit, tourist or business trips for stays up to 90 days. If you intend to stay longer than 90 days, you are required to register at the local Standesamt – Einwohnermeldeamt (Registration Office) within one week of arrival. Citizens of the United States of America may apply for their residence permit after entering Germany without a visa. Alternatively they can apply for a residence permit prior to entry at the German Embassy in Washington or at a German Consulate (currently located in Atlanta, Boston, Chicago, Houston, Los Angeles, Miami, New

York or San Francisco). Inquiries may be made at the German Embassy at <http://www.germany-info.org> . See also Army in Europe Regulation 190-16 and USAREUR 715-2.

15.3 SOFA Contract Clause

INVITED CONTRACTOR OR TECHNICAL REPRESENTATIVE STATUS UNDER U.S. -
REPUBLIC OF KOREA (ROK)

Invited contractor and TR status shall be governed by the U.S.-ROK Status of Forces Agreement (SOFA) as implemented by USFK Regulation 700-19.

- a. Invited contractor or TR status under the SOFA is subject to the written approval of Army Chief of Staff (ACofS), Acquisition Management (FKAQ), Unit #15237, APO AP 96205-5237.
- b. The contracting officer will coordinate with HQ USFK, ACofS, Acquisition Management (FKAQ), IAW FAR 25.8, and USFK Regulation 700-19. The ACofS, Acquisition Management will determine the appropriate contractor status under the SOFA and notify the contracting officer of that determination.
- c. Subject to the above determination, the contractor, including its employees and lawful dependents, may be accorded such privileges and exemptions under conditions and limitations as specified in the SOFA and USFK Regulation 700-19. These privileges and exemptions may be furnished during the performance period of the contract, subject to their availability and continued SOFA status. Logistic support privileges are provided on an as-available basis to properly authorized individuals.
- d. The contractor warrants and shall ensure that collectively, and individually, its officials and employees performing under this contract will not perform any contract, service, or other business activity in the ROK, except under U.S. Government contracts and that performance is IAW the SOFA.
- e. The contractor's direct employment of any Korean-National labor for performance of this contract shall be governed by ROK Labor Law and USFK Regulation(s) pertaining to the direct employment and personnel administration of Korean National personnel.
- f. The authorities of the ROK have the right to exercise jurisdiction over invited contractors and technical representatives, including contractor officials, employees and their dependents, for offenses committed in the ROK and punishable by the laws of the ROK. In recognition of the role of such persons in the defense of the ROK, they will be subject to the provisions of Article XXII, SOFA, related Agreed Minutes and Understandings. In those cases in which the authorities of the ROK decide not to exercise jurisdiction, they shall notify the U.S. military authorities as soon as possible. Upon such notification, the military authorities will have the right to exercise jurisdiction as is conferred by the laws of the U.S.
- g. Invited contractors and technical representatives agree to cooperate fully with the USFK sponsoring agency and RO on all matters pertaining to logistic support. In particular, contractors will provide the assigned sponsoring agency prompt and accurate reports of changes in employee status as required by USFK Regulation 700-19.
- h. Except for contractor air crews flying Air Mobility Command missions, all U.S. contractors performing work on USAF classified contracts will report to the nearest Security Forces Information Security Section for the geographical area where the contract is to be performed to receive information concerning local security requirements.
- i. Invited contractor and technical representative status may be withdrawn by USFK/FKAQ upon:

- (1) Completion or termination of the contract.

(2) Determination that the contractor or its employees are engaged in business activities in the ROK other than those pertaining to U.S. armed forces.

(3) Determination that the contractor or its employees are engaged in practices illegal in the ROK or are violating USFK regulations.

j. It is agreed that the withdrawal of invited contractor or technical representative status, or the withdrawal of, or failure to provide any of the privileges associated therewith by the U.S. and USFK, shall not constitute grounds for excusable delay by the contractor in the performance of the contract and will not justify or excuse the contractor defaulting in the performance of this contract. Furthermore, it is agreed that withdrawal of SOFA Status for reasons outlined in USFK Regulation 700-19, paragraphs 2-6a through 2-6c above shall not serve as a basis for the contractor filing any claims against the U.S. or USFK. Under no circumstance shall the withdrawal of SOFA Status or privileges be considered or construed as a breach of contract by the U.S. or USFK.

16. Contractor Management, Control and Supervision.

16.1 Conduct of Personnel.

The COR, with the approval of the Contracting Officer, may require the contractor to remove from the job site any employee working under this contract for reasons of misconduct or security, or found or suspected to be under the influence of alcohol, drugs, or other incapacitating agents. Contract employees will be subject to dismissal from the premises upon determination by the COR and the Contracting Officer that such action is in the best interests of the Government.

16.2 Prohibited Employees.

The contractor shall not employ any military or civilian employee of the U.S. Government, even in that person's off-duty status, if the employment of that person would be in violation of the Standards of Conduct defined in AR 600-50 or DoD Directive 5500.7, nor shall the contractor employ any such person unless such person seeks and receives approval in accordance with applicable department regulations. The contractor shall not employ any relative of Government military or civilian personnel who has either direct or indirect association with the awarding or administration of this contract. The contractor shall provide the COR with a list of personnel assigned to this contract and their resumes. This requirement shall be updated upon release/replacement of personnel.

16.3 Contractor Behavior in the Workplace.

- Contract employees shall not make final decisions nor approve their own recommendations or the recommendations of other contractors.
- Contract employees shall select and offer personnel who meet the qualifications necessary to perform the tasks in the PWS. Government personnel may review resumes for the purpose of evaluating qualifications. Contractors will be disqualified if their employees participate in the preparation of a PWS or otherwise participate in the development of the requirement. This includes exposure to procurement sensitive information not specifically related to assigned tasks and/or responsibilities as stated in the PWS.
- Contract employees shall identify themselves as contract employees at meetings, in conferences, on the telephone and in electronic mail.
- Contract employees shall not task or supervise government employees nor shall they task or supervise other Contract employees unless specifically required by the PWS. This includes accepting assignments from other contractors or government employees without the approval of a Contracting Officer.
- Contractor personnel shall not represent the Government in discussions or meetings unless approved by the TM, COR, or Contracting Officer.

16.4 Identification of Contractor Personnel.

Contractor personnel must clearly identify themselves as a contractor employee. The name of their company must be part of their email address, all correspondence and all identification badges, desk plates, etc. Additionally, contractor personnel are required to identify themselves as contractor personnel when attending meetings, answering Government telephones, or working in situations where their status as contractor employees may not be obvious.

16.5 Safeguarding Proprietary/Procurement Sensitive Information.

The contractor will not be required to review classified material; however, some material may be considered "Proprietary" or "Procurement Sensitive" in nature and shall be treated accordingly.

- "Proprietary information" is all information, whether disclosed orally, in writings, by drawings, or otherwise, relating to the work to be performed under this contract, whether proprietary to the Government or one of its collaborating partners. Proprietary information includes, but is not limited to, financial information, contract information, properties, formulae, structures, manufacturing processes, and test results. Information ceases to be proprietary when it is generally available to the public or is available from sources other than the Army. All information submitted to the contractor under this contract will be presumed to be Army proprietary.
- Contractor shall safeguard proprietary information both during and after the term of this contract, and shall not appropriate, disclose, or make unauthorized use of proprietary information received under this contract. These requirements include, but are not limited to, the following:
 1. Maintenance of a high degree of physical security over proprietary information at all times;
 2. Discussion of proprietary information only among contractor's employees whose duties and responsibilities require knowledge of that information; and,
 3. Elimination of proprietary information in open publications by the contractor and its personnel.
- Contractor personnel who receive proprietary information shall execute the statement in paragraph d below when this contract becomes effective or when first employed. All statements executed pursuant to this paragraph shall be forwarded to the U.S. Army Medical Research Acquisition Activity when this contract terminates, when the employment ends, or upon request of the Contracting Officer.
 - The following statement shall be executed pursuant to above:

I hereby acknowledge that I have been informed that my duties may require that I have access to proprietary information. I understand this proprietary information which I will receive includes, but is not limited to, financial information, contract information, properties, formulae, structures, protocols, manufacturing processes, and test results.

I agree that I will neither appropriate nor disclose nor make unauthorized use of proprietary information both during and after my employment. I further agree that I will neither include nor draw upon proprietary information received under this contract in open publication. This agreement is executed with the intention that collaborating partners of the United States Government who have submitted information to the Government under non-disclosure obligations shall be third party beneficiary hereunder, and shall have the right to enforce the obligations undertaken herein.

Name: _____

Date: _____

- Contractor shall insert the substance of paragraphs above in each subcontract hereunder. Compliance with the provisions of this clause shall be the responsibility of the contractor.

All data, products, and outputs received, processed, evaluated, loaded, produced, and/or created as a result of this delivery order shall be and remain the sole property of the Government unless specific exception is granted in writing by the Contracting Officer. Performance may require the contractor to access data and information proprietary to a Government agency, another government contractor, or of such nature that its dissemination or use other than as specified on this SOW would be adverse to the interests of the government and/or others. Neither the contractor, nor contract personnel, shall divulge nor release data or information developed or obtained under performance of this SOW, except to authorized government personnel or upon written approval of the Project Director (PD) and/or Contracting Officer (KO). The contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as specified in this SOW. Information identified by the Government staff as sensitive information (Exemption 2 through 9 DoD Privacy Act program: DoD 5400.7-R) shall be handled and processed as For Official Use Only. Information identified as medical quality assurance information (DoD 6040.37) shall be processed as For Official Use Only. Contractor shall comply with RMO Memorandum, "Acquisition Documentation Security Markings", February 15, 1994.

17. Accident/Injury and Incident Reports.

17.1 Safety and Accident Prevention.

Contractor shall conform to the specific safety rules prescribed in AR 385-55 and Army Safety Program in AR 385-10, as applicable. Contractor shall take all reasonable steps and precautions to prevent accidents and preserve the life and health of personnel. Violation of such rules and requirements may be grounds for termination of this contract.

17.2 Security and Fire Prevention Statement.

Contractor shall ensure personnel comply with Army Physical Security Program AR 190-13 and Army Fire Protection and Fire Prevention Program AR 420-90. These regulations can be reviewed at the Fort Sam Houston Fire Prevention and Inspection Branch, Fort Sam Houston, TX. Security regulations are located at the Office of the Provost Marshall, Fort Sam Houston, TX.

18. Project Management.

Management of the project will be as follows:

Contracting Officer's Representative: TBD

Task Manager (TM): TBD

APPENDIX A: ACCEPTABLE USE POLICY AGREEMENT

ACCEPTABLE USE POLICY
& ACKNOWLEDGEMENT OF RESPONSIBILITIES
(Reference Army Regulation 25-2, Appendix B)

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in the United States Army Medical Information Technology Center (USAMITC) network from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. Access. Access to this/these network(s) is for official use and authorized purposes, and as set forth in DOD 5500.7-R (Joint Ethics Regulation), or as further limited by this policy.

3. Revocability. Access to US Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Unclassified information processing. The USAMITC network is the primary unclassified information system for USAMITC.

b. Is a US-only system.

c. Provides unclassified communication to external DOD and other US Government organizations. Primarily, this is done via electronic mail and Internet networking protocols such as *http, ftp, telnet, et al.*

d. Is approved to process UNCLASSIFIED, SENSITIVE information in accordance with DODD 8500.1 (Information Assurance), DODI 8500.2 (Information Assurance Implementation), and AR 25-2 (Information Assurance).

e. And the Internet, as viewed by USAMITC, are synonymous. Email and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

5. Minimum security.

a. Personnel are not permitted access to the USAMITC network unless in complete compliance with the USAMITC personnel security requirement for operating in an Unclassified Sensitive, system-high environment.

b. I have completed "Computer Security Training for Users" and understand the policies presented during that training. I will participate in all training programs as required (i.e., inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect passwords. Passwords will consist of at least 10 characters with two each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords.

d. I will use only authorized hardware and software. I will not install nor use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

- f. I will not attempt to access or process data exceeding the authorized information system classification level.
- g. I will not alter, change, configure, nor use operating systems or programs, except as specifically authorized.
- h. I will not introduce executable code such as, but not limited to, .exe, .com, .vbs, .bat files without authorization, nor will I write malicious code.
- i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the information system and I will not disseminate it to anyone without a specific need to know.
- j. I will not utilize US Army or DOD information systems for commercial financial gain or illegal activities.
- k. Maintenance will be performed by the System Administrator only.
- l. I will use screen locks and log off the workstation when departing the area.
- m. I will immediately report any suspicious output, files, shortcuts, or system problems to the USAMITC Information Assurance Office and I will cease all activities on the system.
- n. I will address any questions regarding policy, responsibilities, and duties to the USAMITC Information Assurance Office.
- o. I understand that--
 - (1) Each information system is the property of the US Army and is provided to me for official and authorized use.
 - (2) Each information system is subject to monitoring for security purposes, and ensures that use is authorized.
 - (3) I do not have a recognized expectation of privacy in official data on the information system and may have only a limited expectation of privacy in personal data on the information system.
 - (4) I should not store data on the information system that I do not want others to see.
 - (5) Monitoring of the USAMITC network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions, or for criminal prosecution.
- p. I understand that in addition to the activities outlined in Army Regulation 25-2, the following activities define unacceptable use of an US Army information system:
 - (1) It is not acceptable to use USAMITC networking services, resources, or facilities for any purposes that violate existing state or federal laws, regulations, policies, or procedures.
 - (2) Data and files on the Internet must be considered copyrighted material and may not be distributed, copied, or published in any form without the written permission of the originator, except as detailed in 17 USC 107 (Copyrights). Material does not need to have a copyright on it to be protected under US Copyright Law.
 - (3) Neither "Spyware" detection, nor "Pop-Up Stopper" software--while the intended protection provided has merit--is authorized for installation on USAMITC computers.
 - (4) Users may not visit illegal or pornographic sites, nor distribute illegal or pornographic material. Sexually related, derogatory, or racially intolerant websites and material are also forbidden.
 - (5) Users may not visit any Internet "chat room" which is not sponsored by USAMITC, the US Army, or the DOD.

(6) Users may not post to any Internet “bulletin board” which is not sponsored by USAMITC, the US Army, or the DOD.

(7) Users may not install, utilize, or participate in any “Instant Messaging” application that is not sponsored by USAMITC, the US Army, or the DOD.

(8) Users may not use USAMITC’s access to the Internet for personal entertainment or financial gain. This behavior includes, but is not limited to, the use of the Internet to--

- (a) Access non-government email accounts.
- (b) Conduct online stock trading, account realignment or internet auction activities.
- (c) Buy, shop, or trade personal goods or services.
- (d) Use the US Army email address as a means to enter contest or sweepstakes drawings.
- (e) Propagate jokes or chain letters through USAMITC email.

(9) Use of the Internet for soliciting money or for advocating a religious or political cause is strictly forbidden.

(10) Users cannot misrepresent themselves or USAMITC.

(11) The use of abusive, vulgar, or objectionable language on the Internet is unacceptable. Additionally, using the Internet for the intentional harassment or harm of an individual or organization is prohibited.

(12) Activities that compromise network security are strictly forbidden, including the disclosure of system IDs, IP addresses, passwords, or any information that could allow the circumnavigation of USAMITC’s security features. This includes, but is not limited to, the use of options such as:

(a) Microsoft’s AutoComplete Function. The AutoComplete feature saves previous entries you have made for Web addresses, forms, and passwords. Then, when you type information in one of these fields, AutoComplete suggests possible matches. These matches can include folder and program names you type in the Address bar, and search queries, or information for just about any other field you fill in on a Web page.

(b) Visiting websites that allow you to send or view electronic greeting cards. Visiting some E-card sites that require the installation of an ActiveX Control causes the generation of a large volume of email. The ActiveX control uses the user’s address book to mail an invitation to the E-card site. The installation of the ActiveX control can include an End User License Agreement that grants permission to use the email contact list.

(c) Unauthorized services (e.g., peer-to-peer, distributed computing, or any application which “shares” USAMITC network resources).

(13) Activities that disrupt or congest USAMITC’s network are forbidden. This includes, but is not limited to, the use of push technologies such as:

- (a) Microsoft’s Subscription Services.
- (b) The PointCast Network.
- (c) The WeatherBug and similar applications.
- (d) Auto-update Stock Market Tickers.

(14) Activities that cause degradation (e.g., excessive consumption of bandwidth) of USAMITC’s network are forbidden. This includes, but is not limited to, the use of technologies such as:

- (a) Streaming Audio and Video.
- (b) Automatic refresh websites (e.g., weather radar) which maintain constant connectivity or automatic refresh capabilities.
- (c) Customizing the format of official USAMITC email by adding stationery (e.g., background texture and color), special fonts, and/or sounds to message traffic.
- (d) Attaching unnecessary or extremely large images to message traffic.

(15) Activities which are authorized and acceptable:

(a) Users are encouraged to use the Internet resources for professional and personal betterment. For example, programmers might use the Internet to read about technical information on computer languages, or perhaps technicians would look at current technological studies. Personal Internet use must meet the legal and regulatory requirements as noted in the preceding paragraphs concerning prohibited activities.

(b) Users are encouraged to use the government email resources responsibly, abiding by normal standards of professionalism and personal courtesy, for periodic contact with family and friends; arranging for personal services (e.g., medical appointments, home repair, et al) during authorized break periods.

Army Regulation 25-2, paragraph 1-1j:

“Military and civilian personnel may be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring implementation of DOD and Army policies and procedures. Violations are identified in bolded text included in the following paragraphs 3-3, 4-5, 4-6, 4-12, 4-13, 4-16, 4-20, and 6-5.

6. Acknowledgement. By signing this document, you acknowledge that you have read the above requirements regarding use of the USAMITC network and understand your responsibilities regarding these systems and the information contained in them. Additionally:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any devices attached to this information system) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:

- The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the U.S. Government may inspect and seize data stored on this information system.

- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.

- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- a. Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
- b. The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
- c. Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
- d. Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- e. A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- f. These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
 - In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
 - All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

APPENDIX B: PRIVILEGED ACCESS AGREEMENT

PRIVILEGED-LEVEL ACCESS AGREEMENT (PAA)
& ACKNOWLEDGEMENT OF RESPONSIBILITIES
(Reference Army BBP 06-PR-M-0003)

I understand that I have access to USAMITC Information Systems (ISs) and that I have and will maintain the necessary clearances and authorizations for privileged-level access.

As a privileged-level user;

I will protect the **root**, **administrator**, or **superuser** account(s) and authenticator(s) to the highest level of data or resource it secures.

I will **NOT** share the **root**, **administrator**, or **superuser** account(s) and authenticator(s) entrusted for my use.

I am responsible for all actions taken under my account and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will **ONLY** use the special access or privileges granted to me to perform authorized tasks or mission related functions. I will only use my privileged account for official administrative actions.

I will not attempt to “hack” the network or connected ISs, subvert data protection schemes, gain, access, share, or elevate permissions to data or ISs for which I am not authorized.

I will protect and label all output generated under my account to include printed materials, magnetic tapes, external media, system disks, and downloaded files.

I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of system or network services, illegal or improper possession of content or files, or the actual or possible compromise of data, files, access controls, or systems to the USAMITC Information Assurance Office (IAO) or, if after hours, to the USAMITC Enterprise Service Desk who will then notify the IAO.

I will **NOT** install, modify, or remove any hardware or software (i.e. freeware/shareware, security tools, etc.) without permission and approval from the USAMITC IAO.

I will not install unauthorized or malicious code, backdoors, software (e.g. games, entertainment software, instant messaging, collaborative applications, etc) or hardware.

I am prohibited from obtaining, installing, copying, pasting, modifying, transferring or using software or other materials obtained in violation of the appropriate vendor’s patent, copyright, trade-secret, or license agreements.

I will not create or elevate access rights of others; share permissions to ISs for which they are not authorized; nor allow others access to IS or networks under my privileged account.

I am prohibited from casual or unofficial web browsing and use of email while using the privileged-level account. This account will **NOT** be used for day-to-day network communications.

I am prohibited from accessing, storing, processing, displaying, distributing, transmitting and viewing material that is; pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.

I am prohibited from storing, accessing, processing, sharing, removing, or distributing Classified, Proprietary, Sensitive, Privacy Act, and other protected or privileged information that violates established security and information release policies.

I am prohibited from promoting partisan political activity, disseminating religious materials outside an established command religious program, and distributing fund raising information on activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g. command social-event fund raisers, charitable fund raisers, etc).

I am prohibited from using, or allowing others to use, Army resources for personal use or gain such as posting, editing, or maintaining personal or unofficial home pages, web-blogs, or blogging sites, advertising or solicitation of services or sale of personal property (e.g. eBay) or stock trading.

I am prohibited from employing, using, or distributing personal encryption capabilities for official electronic communications.

I will contact the USAMITC IAO if I am in doubt as to any of my roles, responsibilities, or authorities.

I understand that all information processed on ISs is subject to monitoring. This includes E-mail and Web Browsing.

I will obtain and maintain required certification(s) in accordance with Army policy to retain privileged level access.

I understand that failure to comply with the above requirements is a violation of the trust extended to me for the privileged access roles and may result in any of the following actions:

- a. Chain of command revoking IS privileged access and/or user privileges
- b. Counseling
- c. Adverse actions under the UCMJ and/or criminal prosecution
- d. Discharge or Loss of Employment
- e. Revocation of Security Clearance

APPENDIX C: CERTIFICATE OF NON-DISCLOSURE

CERTIFICATE OF NON-DISCLOSURE
Disclosure of protected or privileged information
(Reference Army BBP 06-PR-M-0003)

Whoever, being an officer, employee or agent of the United States or of any department, agency or contractor thereof, publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law, any information coming to him/her in the course of their employment or official duties, which information concerns or relates to the trade secrets or proprietary information of a non-Federal government entity; any information protected by the Privacy Act; any information subject to protection under the Freedom of Information Act; other law, regulation, or policy (including all privileged communications such as doctor-patient, attorney-client, etc.); any information protected under the classification system set forth in AR 380-5; or any other information protected by law or regulation (i.e. IG, AAA, CID); shall, in addition to any penalty imposed by said law or regulation, be subject to UCMJ, administrative, or contract remedy enforcement.

CERTIFICATION

I have read the provisions herein and I understand my responsibility not to disclose any matters connected with or pertaining to these provisions as they pertain to the USAMITC network, information systems or components thereof except to persons theretofore listed as having a need to know.

**APPENDIX D: IT PERSONNEL SECURITY DESIGNATIONS AND IA WORKFORCE
CERTIFICATION REQUIREMENTS**

Labor Category	IT Security Designation*	Security Clearance Requirement	IA Management Designation**	IA Technical Designation**	Computing Environment Certification**
Operations Manager	IT-11	N/A	N/A	IAT I	TBD
Administrative Assistant	IT-111	N/A	N/A	N/A	N/A
Scheduler (Level I)	IT-111	N/A	N/A	N/A	N/A
Scheduler (Level II)	IT-111	N/A	N/A	N/A	N/A
Bridge Operator (Level I)	IT-11	N/A	N/A	IAT I	TBD
Bridge Operator (Level II)	IT-11	N/A	N/A	IAT I	TBD
Technical Support Technician (Level I)	IT-11	N/A	N/A	IAT I	TBD
Technical Support Technician (Level II)	IT-11	N/A	N/A	IAT I	TBD
IP Video Network Engineer (Level I)	IT-11	N/A	N/A	IAT I	TBD
IP Video Network Engineer (Level II)	IT-11	N/A	N/A	IAT I	TBD
Wide Area Network Engineer (Level III)	IT-11	N/A	N/A	IAT I	TBD
Database Programmer/Metrics	IT-11	N/A	N/A	IAT I	MCTS-SQL2005
Technical Writer	IT-111	N/A	N/A	N/A	N/A
Videoconferencing Facilitator	IT-111	N/A	N/A	N/A	N/A
* Per AR 25-2					
** Per DoD 8570.01-M					

(End of Summary of Changes)