# New Above Baseline IT Support

# PWS as of 28APR2021:

1. The Contractor shall provide all personnel, management, supervision, equipment, tools, supplies, materials, transportation, and any other items and services necessary to perform the functions of the Performance Work Statement (PWS). The place of performance is Fort Benning Georgia 31905.
2. Inspection and Acceptance. Inspection and acceptance of all work, performance, reports and other deliverables under this contract will be performed at the location specified in this RFP by the Contracting Officer’s Representatives (CORs). CORs are responsible for inspection and acceptance of services under the Contract (TO). The inspection and acceptance is based on the use of the Quality Assurance Surveillance Plan (QASP). The Government will evaluate the contractor’s performance under this TO using the method of surveillance to be identified in the QASP. The Government will record all surveillance observations. When an observation indicates defective performance, the COR will request the contractor's representative to initial the observation.
3. Deliveries or Performance. The anticipated Period of Performance is as follows (or as otherwise stated in the solicitation or contract; contract dates supersede all other dates):

Base Year\* 9DEC 2021 – 8 DEC 2022

Option Year 1 9DEC 2022 – 8 DEC 2023

Option Year 2 9DEC 2023 – 8 DEC 2024

Option Year 3 9DEC 2024 – 8 DEC 2025

Option Year 4 9DEC 2025 – 8 DEC 2026

1. Electronic Submission and Processing of Payment Requests: Electronic invoicing is mandatory in accordance with DFARS 252-232-7003, Electronic Submission of Payment Request. The contractor shall submit invoices via WAWF and the CORs will accept services performed via WAWF. For additional information or if you have questions regarding WAWF, visit the website at https://wawf.eb.mil or contact the Customer Support section at (866) 618- 5988.
2. Special Contract Requirements.
   1. Contractor Manpower Reporting. The Contractor is required to enter data into the Contractor Manpower Reporting (CMR) system. Reporting period will be the period of performance not to exceed 12 months ending 30 September of each year and must be reported by 31 October of each calendar year. Data must be accurate and complete and entered into CMR during the data gathering period of every year, or part of a year, for which the contract is in force. As part of its submission, the contractor will also provide the estimated total cost (if any) incurred to comply with this reporting requirement. NOTE: If the reporting of Manpower Equivalents is not separately priced, insert "NSP" in the blank shown.

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

1. Contracting Office, Contract Contracting Officer, Contracting Officer’s Technical Representative;
2. Contract number, including task and delivery order number;
3. Beginning and ending dates covered by reporting period;
4. Contractor name, address, phone number, e-mails address, identity of contractor employee entering data;
5. Estimated direct labor hours (including sub-contractors);
6. Estimated direct labor dollars paid this reporting period (including sub-contractors);
7. Total payments (including subcontractors);
8. Predominant Federal Supply Class Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each sub-contractor if different);
9. Estimated data collection price;
10. Organizational title associated with the Unit Identification Code is W6CRAAfor the Army Requiring Activity.
11. Locations where contractor and sub-contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website);
12. Presence of deployment or contingency contract language; and
13. Number of contractor and sub-contractor employees deployed in theater this reporting period (by country).
    1. Insurance Requirements. The following kinds and minimum amounts of insurance are required in accordance with FAR clause 52.228-5 entitled, “Insurance—Work on a Government Installation.”

KIND: AMOUNT:

Workmen’s Compensation and Amount required by the State in which this

TO be preformed

Occupational Disease Insurance

Employer’s Liability Insurance $100,000

Comprehensive General Liability $500,000 per occurrence Insurance for Bodily Injury

Comprehensive Automobile Liability $200,000 per person

$500,000 per occurrence for Bodily Injury and $20,000 per occurrence for Property Damage

**Proposal (RFP)** W911SF-19-Above Baseline IT Support

# Attachment 2 – Pricing Schedule (CLIN Structure)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CLIN** | | **Description** | **Quantity** | **Unit** | **Unit Price** | **Amount** |
| 0001 | Services  Base Year | | 12 | Months |  |  |
| 0002 | Services (RMF Requirement as needed) | | 1 | Lot |  |  |
| 0003 | Surge | | 1 | Lot |  |  |
| 0004 | Travel / COST  Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. Travel shall not exceed  $5,000.00 | | 1 | Lot |  |  |
| 0005 | Contractor Manpower Reporting FFP  Contractor shall provide a Contractor Manpower Report as described in the PWS for the period of 28 Mar 2022 – 27 Mar 2023. If not separately price, Contractor shall input “NSP”. | | 1 | Each |  | NSP |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1001 | Services  Option Year 1 | 12 | Months |  |  |
| 1002 | Services (RMF Requirement as needed) | 1 | Lot |  |  |
| 1003 | Surge | 1 | Lot |  |  |
| 1004 | Travel / COST  Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. Travel shall not exceed  $5,000.00 | 1 | Lot |  |  |
| 1005 | Contractor Manpower Reporting FFP  Contractor shall provide a Contractor Manpower Report as described in the PWS for the period of 28 Mar 2023 – 27 Mar 2024. If not separately price, Contractor shall input “NSP”. | 1 | Each |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2001 | Services  Option Year 2 | 12 | Months |  |  |
| 2002 | Services (RMF Requirement as needed) | 1 | Lot |  |  |
| 2003 | Surge | 1 | Lot |  |  |
| 2004 | Travel / COST  Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. Travel shall not exceed  $5,000.00 | 1 | Lot |  |  |
| 2005 | Contractor Manpower Reporting FFP  Contractor shall provide a Contractor Manpower Report as described in the PWS for the period of 28 Mar 2024 – 27 Mar 2025. If not separately price, Contractor shall input “NSP”. | 1 | Each |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3001 | Services  Option Year 3 | 12 | Months |  |  |
| 3002 | Services (RMF Requirement as needed) | 1 | Lot |  |  |
| 3003 | Surge | 1 | Lot |  |  |
| 3004 | Travel / COST  Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. Travel shall not exceed  $5,000.00 | 1 | Lot |  |  |
| 3005 | Contractor Manpower Reporting FFP  Contractor shall provide a Contractor Manpower Report as described in the PWS for the period of 28 Mar 2025 – 27 Mar 2026. If not separately price, Contractor shall input “NSP”. | 1 | Each |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4001 | Services  Option Year 4 | 12 | Months |  |  |
| 4002 | Services (RMF Requirement as needed) | 1 | Lot |  |  |
| 4003 | Surge | 1 | Lot |  |  |
| 4004 | Travel / COST  Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. Travel shall not exceed  $5,000.00 | 1 | Lot |  |  |
| 4005 | Contractor Manpower Reporting FFP  Contractor shall provide a Contractor Manpower Report as described in the PWS for the period of 28 Mar 2026 – 27 Mar 2027. If not separately price, Contractor shall input “NSP”. | 1 | Each |  |  |

**1SF-18-** Above Baseline IT Systems Maintenance Support

# Attachment 3 – Performance Work Statement as of 28APR2021

Performance Work Statement

United States Army Garrison – Fort Benning

Above Baseline Systems Maintenance Support

* 1. **BACKGROUND.** The Directorate of Information Management (DOIM) separated from USAG Fort Benning in 2009, forming the Network Enterprise Command (NEC). Over the past eleven years, our reliance on information technology and the complexity of the information technology systems has increased drastically. In response to new network vulnerabilities, the Defense Information Systems Agency (DISA) continues to increase accreditation requirements. In addition, Installation Management Command (IMCOM) has increased approval requirements for information technology purchases in an effort to ensure all hardware and software systems are compatible and meet the Army’s IT standards. To meet the new requirements of a garrison system maintenance support program, Fort Benning has identified the need for information technology support. Support to the garrison is essential to support force projection and training missions at Fort Benning.

**C.2 Objectives:** The objectives shall include, but not limited to the overall contractor system maintenance support to the Garrison and Garrison Directorates and installation tenant units. The contractor shall perform to the standards in the contract as well as comply with the latest installation, local, state, and federal regulations.

**C.3 SCOPE**. The Contractor shall provide qualified personnel to perform the requirements of information technology system maintenance support to Fort Benning Garrison Commander’s Office and all garrison Directorates, including additional support to the installation tenants units at Fort Benning, GA. The Contractor is responsible for notifying the Contracting Officer (KO) or Contracting Officer’s Representative (COR) of any real or potential deficiencies in personnel availability. This does not, however, relieve the Contractor from meeting the requirements in the performance work statement.

* + 1. **Training.** The Contractor shall ensure contractor personnel are properly trained and that they maintain technical proficiency for the operations and maintenance of the systems and equipment associated with this PWS. Contractor personnel shall have current training and required certifications before beginning work on this task order. The Contractor shall train its own personnel on existing equipment at no cost to the Government. The Government will not provide or fund training to obtain certification for any Contractor employees unless the training is a result of a new requirement.
       1. If during the term of this contract, the Government installs new equipment that requires training to meet the certification requirements of this contract, the Government will provide one- time training during initial fielding and in support of new site activations for those employees currently working on site. The Contracting Officer’s Representative (COR) or Contracting Officer (KO) will approve all training in advance. If the Contractor replaces an employee who has received Government-provided training as described above for any reason, the Contractor shall provide any needed training at no cost to the Government.
       2. Training Records. The Contractor shall ensure required training is documented within records that are available upon request by the KO or COR.
    2. Hours of Operation. The Contractor shall provide services during the hours ranging between 0700 – 1700 (depending on the area of assignment), Monday – Friday, except on federal holidays as designated by the Office of Personnel Management at <http://www.opm.gov/policy-> data-oversight/snow-dismissal-procedures/federal-holidays/#url=Overview or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.
       1. **Overtime.** Services to be performed under this contract are generally performed during normal duty hours. Periodically, requirements including emergencies, special projects, supporting deployments, and seasonal requirements, may require work be accomplished at times other than normal duty hours. After hour maintenance of life safety systems may be required on an as needed basis. These systems are identified in the Performance Work Statement.

**C.3.3 Information Technology (IT) Software and Equipment.** The Contractor shall request project-related IT software, equipment and tools in support of the task order requirements through the COR. COR will assist with locating the Army approved list with all Information Assurance approvals, Certificate of Networthiness (CoN), and Joint Interoperability Test Command (JITC) certifications. This software/equipment shall require IAVA scanning and patching and compliance with applicable DISA Security Technical Implementation Guides (STIG) to the degree applicable prior to allowing connectivity to the Government production network, by the contractor.

**C.3.3.1** The Contractor shall ensure that a Government CoN is available for all Contractor-purchased software and IT equipment that will be installed or integrated into existing government IT systems and networks. The Contractor shall first check the U.S. Army Network Enterprise Technology Command (NETCOM) web site at <https://netcom.army.mil/vendor/Compliance.aspx> for a list of systems and commercial-off-the shelf (COTS), Government-off-the shelf (GOTS), or other equipment with current valid CoNs. The Contractor must be registered in AKO by the COR for access. If a CoN is not available, The Contractor shall fill out and submit the applicable Networthiness Checklist to the COR.

**C.3.3.2 Purchases.** The Contractor shall submit a list of items required and a cost analysis to the COR or KO for approval prior to any purchase. The Contractor shall only purchase materials directly related to the maintenance support and necessary to accomplish and assure acceptable levels of O&M for supported systems. The Contractor shall purchase materiel necessary to complete assigned special projects and for maintenance of bench stock levels, expendable supply levels or requirements for routine O&M maintenance outlined in the task order. All non- expendable items purchased shall become the property of the Government and added to the list of Government-furnished property (GFP). Approved purchases will be reimbursed on the Supply CLIN not to exceed (NTE) $2.5M.

**C.3.4** **CONTRACTOR ACCOUNTABILITY**

**C.3.4.1** **GENERAL**

The government will provide the facilities, utilities, equipment, materials, and supplies described herein as government-furnished property. Government-furnished property (GFP) consists of government-furnished facilities (GFF), government-furnished equipment (GFE) (to include automated data processing equipment (ADPE) and government-furnished parts, materials, and supplies, placed in the contractor’s custody. The government will also provide certain services to the contractor. The contractor shall not use GFP or services for any other purpose than execution of work under this contract. The contractor shall loan GFP to government operations and/or other government contractors when directed by the KO. The contractor shall assume responsibility for GFP provided for his/her use and shall take precautions to prevent fire and safety hazards, odors, chemical spills, and vermin. At the completion of the contract, GFP shall be returned to the government in the same condition as received, except for reasonable wear and tear.

**C.3.4.1 Report of Government Property**

The contractor shall prepare and submit to the KO an annual report of government property on Department of Defense (DD) Form 1662, and according to the requirements of the contract.

**C.3.4.2** **Removal of Property**

The contractor shall not remove GFP from the installation or other supported areas without written approval from the Government Property Administration Office (Property Book Holder). Department of the Army Form 2062, Hand Receipt/Annex Number, shall be used to obtain Property Administration Officer approval for the removal of GFP from the installation.

**C.3.5 Security and Background Check Requirements**. Contractor performance includes, but is not limited to,installation, operation, and maintenance of unclassified and classified systems, networks, devices and equipment; work in classified, sensitive, and/or Restricted Areas where exposure to classified information cannot be precluded and/or where security clearances are required. The Contractor shall, at a minimum, have a final Secret facility clearance level (FCL) at time of contract award.

**C.3.5.1** All Contractor personnel performing on this task order must be U.S. citizens with required security clearance or suitability investigations. Upon task order start date, all contractor personnel shall possess and maintain the required security clearance over the life of the TO in with DD Form 254, Contract Security Classification Specification. After TO award, newly hired personnel who require a security clearance for this work effort shall have submitted for a security clearance within two (2) months of being hired and shall maintain the required security clearance throughout employment on this TO. Contractor personnel who require a Secret security clearance and who will be performing IT-I functions will require a ANACI/NACLC or equivalent completed with suitability determination for IT level II access. The Contractor shall contact the supporting Government Security Office/G-2/S-2 for submission of the ANACI/NACLC or equivalent (SF 86) via the Army Investigative Enterprise Solution (AIES). The SF 86 will indicate SECRET access/IT level II. The Contractor shall provide the contract/TO number as authority to request the investigation. Contractor interim privileged level access to Army systems prior to completion and favorable adjudication of the required investigation will be in accordance with AR 25-2. If contractor personnel have a current ANACI/NACLC or equivalent on record in JPAS, the AR 25-2 investigative requirement for IT Level II is satisfied. Contractor personnel who do not require a security clearance but who require an investigation for suitability/trustworthiness purposes shall have SUBMITTED the required investigation documentation within two (2) months after TO award. Contractor personnel shall comply with all applicable security and safety regulations, guidance, and procedures, including local, referenced in the PWS and in effect at the work sites. The Contractor shall coordinate with the supporting Government security office for submission of required suitability investigations.

**C.3.5.2 Access and General Protection/Security Policy and Procedures**: Contractor and all associated sub-contractors employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by the government representative). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by Installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

**C.3.5.3** The Contractor shall protect Government information, systems/networks, devices, and other Government-furnished equipment and property, based on the level of access provided to contractor personnel supporting this contract. The Contractor shall comply with and enforce all security and information assurance requirements and measures, as specified in applicable directives and as stated in the task order.

**C.3.5.4** Contractor/Sub-Contractor employees providing services under contracts are subject to the following process:

**C.3.4.5**  Each employee (direct employee and sub-contractor employee) working under this contract who has contact with children under 18 years of age, shall be screened with the appropriate background checks as governed by the Army Directive 2014-23 “Conduct of Screening and Background Checks for Individuals Who Have Regular Contact with Children in Army Programs”, dated 10 September 2014. A copy of the Army Directive can be found at http://www.apd.army.mil/pdffiles/ad2014\_23.pdf. The background check requirements for Contractors can be found in Enclosure 3 – Screening and background checks for appropriated and non-appropriated fund personnel, military personnel, foreign national employees overseas, and contractors.

**C.3.4.6** Background checks will be initiated and paid for by the Government. The cost for the pre-employment screening is the responsibility of the Contractor. The Commander Designated Entity (CDE) at the Installation supports IMCOM by coordinating, submitting, tracking child related background checks, and reviewing and compiling the results to identify whether they contain derogatory information to be passed on for a suitability determination. The CDE will advise and assist CONTRACTOR and sub-CONTRACTOR employees completing all required documents required for the background-check process. CDE contact information will be provided upon contract award.

**C.3.4.7** Additional information on the background check process can be found at:

[http://www.opm.gov/investigations/background-investigations.](http://www.opm.gov/investigations/background-investigations)

**C.3.4.8** Re-verification (IRC and FBI fingerprint check) is required every 5 years.

# 

# C.3.6 Information Assurance.

**C.3.7 For Information Assurance (IA)/Information Technology Training.** All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoD 8570.01, DoD 8570.01-M and AR 25-2 within six months of appointment to IA/IT functions.

**C.3.7.1** **Army Training Certification Tracking System (ATCTS) registration for contractor** **employees who require access to government information systems:** All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the information system and then annually thereafter.

**C.3.7.2 Global Address Listing (GAL):** All contract employees who require access to Government Information Systems shall update their profile and Global Address Listing (GAL) information: https://www.dmdc.osd.mil/milconnect within 10 working days of being granted IT access**.**

**C.3.8 Information Assurance Workforce Certification.** Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.239-7001 (Information Assurance Contractor Training and Certification) applies to this task order. This task order is subject to the mandates of DoD 8570.01-M, which establishes baseline technical and management IA skills for personnel performing IA functions within DoD. Functions spanning multiple levels require certification of the highest level functions. Contractor personnel performing functions in multiple categories or specialties shall hold certifications appropriate to the functions performed in each category or specialty.

**C.3.8.1** The Contractor shall ensure its IA workforce members have the baseline certifications corresponding to their IA functions, as defined in Chapters 3, 4, 5, 10, and 11, and Appendix 3 of DoD 8570.01-M at work performance start date. Contractors will obtain all required Computing Environment (CE) certificates within 6 months of being engaged. The IAT Level I baseline certification is the minimum requirement for unsupervised privileged general protect. Contractor certification holders shall ensure that their certificates remain active and are renewed prior to expiration.

**C.3.8.2** Contractor IA certification holders shall release their certification information to the Department of Defense through the Defense Workforce Certification Application, [https://www.dm](http://www.dmdc.osd.mil/appj/dwc/index.jsp)dc.osd.m[il/appj/dwc/index.jsp.](http://www.dmdc.osd.mil/appj/dwc/index.jsp)

**C.3.8.3** Table 1 reflects the Personnel Security (IT Level) and IA Workforce Specialty requirements, aligning the IA functional responsibilities and access levels to the task order tasks, in accordance with DoD 8570.01-M.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IT Level**  **IAW AR 25-2,**  which identifies requirements for IT level designations and security investigation requirement for each level ) | **IA Category & Level**  **IAW DoD 8570.01-M,** which  identifies required DOD acceptable Baseline Certifications); BBP (Better Business Practice) on Information Assurance Training and Certification, 05-PR-M-0002, identifies Army minimum required training for the same IA category and level) | **Clearance Required** | **BI**  **Require d** | **Computing Environment Certifications** |
| IT-I | IAT-III | SECRET | SSBI | Yes |
| IT-I | IAT-II | SECRET | SSBI | Yes |

Table 1. Listing of positions with Information Assurance and Security Requirements

**C.3.8.4** **Non-Government-owned computing systems or devices.** The Contractor shall comply with AR 25-1 and AR 25-2. The Contractor shall not install or connect non-Government-owned computing systems or devices to Government networks without the COR’s coordinating and obtaining proper authorization from the appropriate Information Assurance Program Manager (IAPM), ensuring that all software has a Government Certificate of Networthiness. The non- Government-owned computing systems or devices include, but are not limited to, personal or contractor-owned thumb drives (e.g., memory sticks, flash drives, Universal Serial Bus (USB) drives, jump drives, pen drives), removable or external hard drives, Personal Digital Assistants (PDA), PC Cards/Express Cards, MP3 players, cell phones, smartphones, Blackberries, digital media, floppy disks, compact disc (CD)/digital video disk (DVD) burners, optical recordings, photo flash cards, mobile device (laptop or tablet), or any devices that can store data.

**C.3.8.5** Protection of Sensitive Unclassified Data. The Contractor shall ensure any sensitive information, including, but not limited to, Personally Identifiable Information (PII) and Controlled Unclassified Information (CIU), proprietary, and Law Enforcement Sensitive information residing On Mobile Computing Devices (MCD) or other external media, is protected in accordance with current Data at Rest (DAR) guidelines and requirements. The Contractor shall use an authorized, approved, and prescribed DAR solution. The MCDs include, but are not limited to, laptop, netbook, notebook, or tablet computers, and Blackberry or equivalent devices. External media include optical disk media such as CDs, DVDs, USB drives (also referred to as flash or thumb drives) (when authorization to use them is restored), floppy disks, and other portable digital storage devices. Guidance for protecting DAR information appears in DoD Policy Memorandum, 3 Jul 07, subject: Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Media, and DoD Component implementing instructions.

# C.3.9 Anti-Terrorism/Force Protection Security Requirements.

**C.3.9.1 Antiterrorism Level I Training.** The Contractor shall ensure that all contractor employees, including subcontractor employees, requiring access to Army installations, facilities, or controlled access areas complete Antiterrorism (AT) Level I awareness training within 30 calendar days after start of employee performance on this task order. Within 5 calendar days of training, The Contractor shall certify to the COR or KO that all employees performing work under this task order have completed the AT Level I awareness training. AT Level I awareness training is available at https://jkodirect.jten.mil, course #JS-US007-14 to receive credit for the training.

**C.3.9.2** **iWATCH** The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Anti-Terrorism Training Officer). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.

**C.3.9.3** During declared emergencies, natural disasters, epidemics, pandemics, quarantine, and/or elevated Force Protection Conditions (FPCONs) Charlie or Delta, contractor performance under this task order shall be determined by the COR or KO. All contractor employees providing services under this task order are required to report for duty as scheduled and remain on duty during declared emergencies and/or elevated FPCON levels unless otherwise directed by the KO or COR.

**C.3.10 Operations Security (OPSEC).** Operation Security (OPSEC) training: In accordance with AR 530-1 all personnel, to include contractor employees and associated sub-contractor employees must complete Level I Operations Security (OPSEC) training which is composed of both initial and continual awareness training (annually). All personnel within the first 30 days of arrival in the organization must receive initial training to include a briefing on the organizations critical information read/sign the OPSEC Individual User Compliance Agreement form. The end state of initial and continual awareness training is that each individual should have CAC the requisite knowledge to safeguard critical information. The Contractor is not required to prepare an OPSEC Plan. The contractor shall adhere to the Government's Operations Security (OPSEC) Standard Operating Procedure (SOP)/Plan during the entire period of performance. The Contractor shall comply with DoD Directive 5205.02E, Army Regulation 530-1, and the requiring activity OPSEC program. The Contractor shall maintain all OPSEC training records and shall provide copies to the COR upon request.

**C.3.11 Visit Authorization Letter:** The Contractor must provide a valid (IAW DoD 5220.22-M) Visit Authorization Letter (VAL) for every employee on the contract, prior to their visit. This VAL must be originated by the Contractor's Security Office (also called Facility Security Officer or FSO), and shall be sent to the Contracting Officer Representative or Security Representative. The VAL must include the purpose and date(s) of visit, security clearance information, social security number, the contract number. This request is valid for up to one year. The request must be reviewed and updated as needed, but at least annually.

**C.3.12 Statement of Non-Disclosure:** All Contractor personnel will comply with the non- disclosure requirements in the clause at FAR Part 52.227-14 (or DFAR equivalent). All Contract Personnel must sign a statement of non-disclosure.

**C.3.13 Handling or Access to Classified Information**: Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified “Confidential,” “Secret,” or “Top Secret” and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

**C.3.14 Threat Awareness Reporting Program:** For all contractors with security clearances. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b.

**C.3.15 Physical Security**: The Contractor shall be responsible for safeguarding all Government equipment, information and property provided for Contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

**C.3.16 Key Control**: The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer.

**C.3.16.1 Keys:** In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re- keying or the replacement of the lock or locks shall be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

**C.3.16.2 Prohibited Use of Keys:** The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor’s employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

**C.3.16.3 Lock Combinations:** The Contract or shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor’s Quality Control Plan.

**C.3.17 Accounting for Contractor Support.** The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where The Contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this task order The contractor is required to completely fill in all the information in the format using the following web address: https://cmra.army.mil. The required information includes: (1) Contracting Office, Contracting Officer, Contracting Officer's (Technical) Representative; (2) Contract number, including task or delivery order number; (3) Beginning and ending dates covered by reporting period; (4) Contractor name, address, phone number, e-mail address, identity of contractor employee entering data; (5) Estimated direct labor hours (including subcontractors; (6) Estimated direct labor dollars paid this reporting period (including subcontractors); (7) Total payments (including subcontractors); (8) Predominant Federal Service Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each subcontractor if different); (9) Estimated data collection cost; (10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information); (11) Locations where the contractor and subcontractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website); (12) Presence of deployment or contingency contract language; and (13) Number of contractor and subcontractor employees deployed in theater this reporting period (by country). As part of its submission, The Contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance not to exceed 12 months ending September 30 of each Government fiscal year and must be reported by 31 October of each calendar year. Contractors may use a direct XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the web site. The specific formats for the XML direct transfer may be downloaded from the web site.

The Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Army via the eCMRA secure data collection site. The contractor is required to completely fill-in all required data fields within the eCMRA. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk at: [http://www.ecmra.mil.](http://www.ecmra.mil/)

**C.3.18 Contractor Identification Requirements.** In accordance with FAR subpart 37.114(c), all Contractor personnel attending meetings, answering Government telephones, and working in other situations where their Contractor status is not obvious are required to identify themselves as such to avoid being mistaken for Government officials. Contractors performing work at Government workplaces shall provide their employees with an easily readable identification (ID) badge indicating the employee’s name, the Contractor’s name, the functional area of assignment, and a recent color photograph of the employee. Contractors shall require their employees to wear the ID badges visibly when performing work at Government workplaces. Contractor personnel must also ensure that all e-mails, documents, or reports they produce are suitably marked as Contractor products and/or that contractor participation is appropriately disclosed. All signature blocks on e-mails shall indicate that the sender is a Contractor employee and include the Contractor's company name.

**C.3.18.1** **Common Access Card (CAC).** For contractors requiring Common Access Card (CAC): Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

**C.3.19 Quality Control.** The Contractor shall develop and maintain an effective quality control plan to ensure services are performed in accordance with this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor’s quality control program is the means by which he assures himself that his work complies with the requirement of the contract. The Quality Control Plan (QCP) is to be delivered, within 30 days after contract award, and within 5 working days when changes are made thereafter. The Offeror’s QCP must be detailed, containing a systematic approach to monitor daily operations of key and essential functions for providing quality service to the Government, i.e. discrepancy identification procedures, corrective action procedures, prevention procedures for occurrence/re-occurrence of discrepancies, trend analysis usage, and customer feedback utilization. Such QCP requirements will increase the likelihood of successful contract performance. After acceptance of the quality control plan the Contractor shall request the contracting officer’s acceptance in writing of any proposed change to his QC system.

**C.3.19.1 Quality Assurance.** The Government shall evaluate the Contractor’s performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

**C.3.20 Data Rights.** The Government has unlimited rights to all documents/material produced under this task order. All documents and materials, to include the source codes of any software, produced under this task order shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

**C.3.21** **Post Award Conference/Periodic Progress Meetings.** The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The Contracting Officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the Contracting Officer will apprise the Contractor of how the government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

**C.3.22 Task Order Contracting Officer Representative (COR).** The (COR) will be identified by separate letter. The COR monitors all technical aspects of the task order and assists in task order administration The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the task order: perform inspections necessary in connection with task order performance: maintain written and oral communications with the Contractor concerning technical aspects of the task order: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

**C.3.23 Key Personnel**. The contractor shall provide a Contract Manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor during absences shall be designated in writing and provided to the Contracting Officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The Contract Manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The Contract Manager or alternate shall be located at Fort Benning and be available between 0700-1700, Monday through Friday except Federal holidays or when the government facility is closed for a pandemic, or administrative reasons. Fort Benning Garrison requires that the individual who will serve as the contract manager will have a minimum of 5 years’ experience in a technical environment with 5 years supervisory experience managing projects or programs of similar scope and size either for the Government or on behalf of a Government client. Individual will have an Active SECRET Clearance in good standing on the first day of this contract, from start of Period of Performance. Project Management Professional (PMP) certification is required. The Contractor shall submit resumes for key personnel in the management and staffing section of the technical proposal. Key personnel are identified as the contract manager, alternate contract manager, and those individuals responsible for managing the work in each functional area of the Contract. Any changes to the working status of these key personnel shall be provided to the KO for approval within five working days prior to the change.

**C.3.24** **Government Driver’s License**: All full-time contractor employees shall be required to acquire a Government Driver’s License to drive government-owned or government-leased vehicles. This must be acquired with 30 calendar days of hire. Proof of driver’s license shall be turned in to the COR upon issuance of license.

**C.3.25 Conservation of Utilities:** The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities which includes turning off the water faucets or valves after using the required amount to accomplish the necessary cleaning.

**C.2.26** **Telephone Usage:** Contractor employees shall not use Government telephones at the work site for personal reasons or make any toll or long distance calls.

**C.3.27 Applicable Documents** The following publications form a part of this contract. All publications below in which the Contractor shall comply are “Mandatory.” The Contractor shall use current commercial practices and publications whenever possible. A significant number of Army regulations that govern the conduct of the required work are listed below. The PWS may set a higher standard of performance than an applicable Army regulation. The PWS will control over the regulations unless a particular PWS provision is in direct conflict with the applicable provision of the Army regulation. The publications can be accessed from internet site [www.apd.army.mil.](http://www.apd.army.mil/) The Government will provide those publications not available on a web site. The Contractor shall comply with changes to publications. The Contractor shall inform the KO of any changes to a publication or documents that impact the cost of the task order.

Technical Bulletins (TB)

* TB 43-180 Calibration and Repair Requirements for the Maintenance of Army Material
* TB 380-41, Security: Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material (FOUO requires AKO access)
* TB 385-4 Safety Requirements for Maintenance of Electrical and Electronic Equipment Department of the Army Pamphlets (DA PAM)
* DA Pam 25-1-1 Army Information Technology Implementation Instructions
* DA Pam 710-2-1 Using Unit Supply System (Manual Procedures) Department of the Army (CIO/G-6) Policies
* Army CIO/G-6 List of Directorate of Information Services (NEC) Service Level Agreement (SLA)/Operational Level Agreement (OLA) (Implemented by the Secretary of the Army (Office, Chief Information Officer, via Memorandum, SUBJECT: Army Command, Control, Communications, Computers, and Information Management (C4IM) Service List, dated 5 Nov 2014. (Available from the NEC)
* Army Information Technology Metrics Program (available from the NEC) Department of the Army Regulations (AR)
* AR 25-1, Army Information Technology
* AR 25-2, Information Assurance
* AR 25-55, The Department of the Army Freedom of Information Act Program
* AR 25-400-2, The Army Records Information Management System (ARIMS)
* AR 190-13, The Army Physical Security Program
* AR 190-51, Security of Unclassified Army Property (Sensitive and Non-sensitive)
* AR 350-1, Army Training and Leader Development
* AR 360-1, Army Public Affairs Program
* AR 380-5, Department of the Army Information Security Program
* AR 380-27, Control of Compromising Emanations (FOUO requires AKO access)
* AR 380-40, Safeguarding and Controlling Communications Security Material (FOUO requires AKO access)
* AR 380-49, Industrial Security Program
* AR 380-67, Personnel Security Program
* AR 381-12, Threat Awareness and Reporting Program
* AR 385-10, The Army Safety Program
* AR 525-13 Antiterrorism (FOUO requires AKO access)
* AR 530-1 Operations Security
* AR 735-5, Property Accountability Policies
* AR 750-1, Army Materiel Maintenance Policy
* AR 750-43, Army Test, Measurement, and Diagnostic Equipment

# Army and DoD Memoranda and Other Documents

* DA Pam 25-1-1, Army Information Technology Implementation Instructions
* DISA Cir 300-115-3, Defense Information System Network (DISN) Secret Internet Protocol Routing Network Security Classification Guide
* DoDM 5200.01-V1, DoD, Information Security Program: Overview, Classification, and Declassification
* DoDM 5200.01-V4, DoD Information Security Program: Controlled Unclassified Information (CUI)
* DoDI 8500.01, Cybersecurity
* DoDI 8500.2, Information Assurance (IA) Implementation
* DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP)
* Department of the Army Memorandum, 13 August 2008, subject: Clarification on Personnel Security Investigative Requirements for IT Positions
* **Army CIO/G-6 Best Business Practice 05-PR-M-0002, Information Assurance (IA Training and Certification (available at** https://informatioinassurance.us.army.mil/bbp/index.php **(Requires AKO Access)**
* **Committee on National Security Systems Instructions (CNSSI) 4009, National Information Assurance Glossary (available at** <http://www.cnss.gov/full-index.html>**)**

# Message, Department of the Army CIO/G-6, (ALARACT 293/2007), dated 261800Z Dec 07, subject: Implementation of Standard DoD IA Awareness Training (available from the Government requiring agency)

* DOD Policy Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Media, dated 3 Jul 2007 and DOD Component implementing instructions
* DoD Directives (DoDD) (available at <http://www.dtic.mil/whs/directives)>
* DoDD 5205.02E, DoD Operations Security (OPSEC) Program
* DoDD 5400.11, DoD Privacy Program
* DoDD 8100.2, Use Of Commercial Wireless Devices, Services, And Technologies In The Department Of Defense (DOD) Global Information Grid (GIG)

DoD Manuals

* DoD 5220.22-M, National Industrial Security Program Operating Manual
* DoD 8570.01-M, Information Assurance Workforce Improvement Program Code of Federal Regulations (CFR)
* 15 CFR Part 700, Defense Priorities and Allocations System (DPAS)
* \*47 CFR Part 68, Connection of Terminal Equipment to the Telephone Network
* \*47 CFR Part 76, Multichannel Video And Cable Television Service, Subpart K, Technical Standards.

Telecommunications Industry Association (TIA)/Electronic Industry Association (EIA) Standards/American National Standards Institute (ANSI) Standards

* \*TIA 102 Series, Suite of Standards to support the Land Mobil Radio Network
* \*TIA-232-F, Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange
* \*EIA-310-D, Cabinets, Racks, Panels, and Associated Equipment
* \*TIA/EIA-472-0000-A, Generic Specification for Fiber-Optic Cables
* \*ANSI/TIA-472C000-B, Standards for Optical Fiber Premises Distribution Cable
* TIA/EIA-472D000-A, Sectional Specification for Fiber-Optic Communications Cables for Outside Plant Use
* \*TIA-4920000B, Generic Specification for Optical Waveguide Fibers
* \*TIA/EIA-60-6A, Administration Standard for Commercial Telecommunications Infrastructure
* \*TIA/EIA-568-B Series, Commercial Building Telecommunications Cabling Standard
* \*TIA/EIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces
* \*TIA-603-C, Land Mobile FM or PM Communications Equipment Measurement and Performance Standards
* \*TIA/EIA-422-B, Electrical Characteristics of Balanced Voltage Digital Interface Circuits
* \*EIA-440-B, Fiber-Optic Connector Terminology
* \*TIA/EIA-530-A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector
* \*TIA/EIA-455-B, Standard Test Procedures for Fiber-Optic Fibers, Cables, Transducers, Sensors, Connecting and Terminating Devices, and Other Fiber-Optic Components

OSHA Standards

* 29 CFR Part 1910.146, Permit-required Confined Spaces
* \*29 CFR Part 1910.268, Telecommunications

NETCOM Regulations (requires CAC access) https://army.deps.mil/NETCOM/sites/G1/PolPubsForms/Pages/Regulations.aspx

* NETCOM Regulation 25-56 Personally Identifiable Information
* NETCOM Regulation 25-70 Web Content Administration, Policies, and Procedures
* NETCOM Regulation 380-5 Information Security
* NETCOM Regulation 385-1 Safety and Occupational Health
* NETCOM Regulation 750-1, Maintenance Guidance and Concepts
* NETCOM Regulation 750-2, Battery Management Program
* NETCOM Regulation 750-8, Army Test, Measurement, and Diagnostic Equipment Program

# C.4 SPECIFIC TASKS:

**C.4.1 Garrison IMO Support**: The primary place of performance will be Camp Merrill, Building 4 and outlying Garrison directorates within Fort Benning, GA. The Contractor shall:

•On this contract a SECRET security clearance is required by every contractor upon hiring.

•Provide Active Directory Management on user and computer accounts, print objects, and security groups; create and maintain standard computer account naming conventions.

•Provide on-site and remote customer and automation support for 2000 Garrison personnel.

•The contractor will assist the Garrison IMO with duties as defined by AR 25-1, DA PAM 25-1-1 and AR 25-2, to include all Garrison IT related procurement records and approvals.

•Coordinate with the Garrison Directorate Information Management Officers (IMOs) to develop a Strategic plan for the cyclical replacement of all types Information Technology equipment (network, hardware, software, communications, and video teleconference rooms). The plan shall be in accordance with AR 25-1 and DA PAM 25-1-1.

•Develop and enhance business process development for day-to-day maintenance and support requests. Work with the Network Enterprise Center to resolve issues related to user accounts, network outages, remote access and Wi-Fi access. Provide incident response for systems/users with known or suspected Information Assurance compliance issues.

•Assist the Information Assurance Security Officer (IASO) in accordance with AR 25-1, DA PAM 25-1-1, and AR 25-2 to include establishing and maintaining a record of all Garrison above baseline software in both hard copy and digital format on the SharePoint Portal. This is deemed a Mission Assurance Category (MAC) II function.

•Operate and maintain hardware and software associated with standard IT service delivery; implement and maintain all prescribed configurations (e.g., Security Technical Implementation Guide (STIG)); and integrate operations with internal and external activities (e.g. Regional Cyber Center (RCC), 7th Signal Command (Theatre) G3 Operations, etc.).

•Provide expert advice by identifying IT service delivery issues and potential shortfalls with proposed technical solutions; engineer/re-engineer technical solutions to address identified solutions design shortfalls; provide life-cycle management consultation and advice.

•Execute system deployments and technical changes on a quarterly or as required basis as determined by Security Technical Implementation Guide, Microsoft and other vendor based product rollout schedules or as required by Army, Defense Information Systems Agency or other agency. Recommend, develop and maintain operational processes and automated solutions.

•Provide IT performance metrics/service reporting and documentation, weekly IT Service Delivery reports, monthly contract quality performance and quarterly Installation Status Report (ISR) processes. Ensure 99.9% service availability.

**C.4.2 Above Baseline System Administration:** The contractor shall receive, review, and repair all deficiencies noted in the IT Vulnerability Report generated by the Department of Defense on a monthly basis as it applies to the systems associated with Fort Benning. This may require access to sensitive information and must be treated with appropriate security protocols to ensure that contractor personnel are appropriately cleared. This report is considered by the Government as Classified and will be reviewed at the government facility. Fort Benning Security / MCoE G-2 appointed Courier(s) will check out the Vulnerability Report from government control and courier report to an area containing the server that requires patches. All classified material handling rules will be strictly enforced by TSS Courier(s). The classified report will be returned to government control when work is completed, or at the end of each day. The contractor shall:

•Manage and perform maintenance on servers, provide print server coordination to maintenance and management for MFP devices.

•Maintain all applicable software licenses and maintain updated software Certificates of Networthiness (CoN).

•Develop and maintain network diagrams, data flow charts, Tenant Security Plan, Contingency Plan and Configuration Management Plan for up to 35 Garrison IT Systems. These documents and diagrams will be stored on the Installation SharePoint.

•Perform Systems Administration for all (is exhibit referenced inclusive) above baseline systems. The Contractor shall prepare systems for Designated Approving Authority (DAA) and manage Authority To Operate (ATO) and Authority to Connect (ATC). The Contractor will also provide DISA Platinum Security Technical Implementation Guide (STIG) standard. The Contractor shall evaluate the automated report produced by the scanning software and implement corrections.

•The Contractor will provide assistance to current databases, future integration of databases and\or systems that may contain databases to function, contractor assistance may include capacity planning, installation, configuration, database design, migration, performance monitoring, security, troubleshooting, as well as backup and data recovery.

•Contractor Shall Audit AUP and IA directories to ensure 100% DoD IA compliance. Conduct quarterly Security Technical Implementation Guide (STIG) analysis and mitigation on servers to ensure DoD IA compliance.

•Assist the Information Assurance Security Officer (IASO) in accordance with AR 25-1, DA PAM 25-1-1, and AR 25-2 to include establishing and maintaining a record of all Garrison above baseline software in both hard copy and digital format on the SharePoint Portal. This is deemed a Mission Assurance Category (MAC) II function.

•Provide a summary report on server space availability

**C.4.3 Development of New IT Solutions:** Primary place of performance is building 4, Fort Benning, GA. On average, 2000 users will be supported annually (to include Active Directory object creation, deletion, activation and deactivation. Mobile/Desktop devices (laptop, tablet, workstations) image and any associated re-image due to hardware failure, image breakage etc.), For every local service support ticket that requires NEC support a separate Army Enterprise Service Desk (AESD) service ticket number will be documented and tracked to completion. The Contractor shall:

* •Research existing IT processes and recommend efficiency and effectiveness improvements.
* •Research available Commercial of the Shelf (COTS) IT solutions and provide recommendations. If a COTS is not feasible, the Contractor shall research other design options and recommend solutions to the Garrison IMO.
* •Assist the Garrison IMO with IMCOM’s monthly IT Governance Board for all new COTS and/or internally developed solutions. Support will include, but not limited to, IT system information, IT hardware specifics, and IT software specifications as required by the COR.
* •Provide on-going review of Standard Operating Procedures & Tenant Security Plan, suggesting updates as required by mission changes and recommended efficiencies.
* •Assist the Garrison IMO with project management and technical advisement on Garrison Command pilot projects.
* •Assist the Garrison IMO by acting as Garrison Command representative in projects under taken by units under Garrison Command.

**C.4.4 G-6 Audio / Visual - Video Teleconferencing Support:** The Contractor shall provide secure and non-secure customer support services for the Garrison VTC suites located across the Fort Benning, GA installation campus. The primary place of performance is building 4, Fort Benning. While the Contractor shall primarily provide telephonic or remote support for geographically separated locations such as Camp Merrill, and Garrison directorates throughout Fort Benning. The Contractor may be required to travel to one of the Garrison directorates on Fort Benning such as. If travel to any of these locations is required, the contractor must submit in writing, a request for approval to the COR at least five days in advance of the requested travel date. At a minimum, the request must include number of personnel traveling, numbers of days, anticipated lodging costs, meals, car rentals or mileage. Costs cannot exceed established Joint Federal Regulations (JFR) for Travel guidelines. Emergencies will be handled on a case-by-case basis, and can be initiated with a phone call.

However, the contractor is required to follow-up with a written request.

* •Establish and maintain an up-to-date database to track VTC suites to include inventory by unit, IP, location, POC, Site ID, etc.
* •Update software and firmware versions on all VTC equipment and similar replacement equipment; test updated equipment to validate proper functionality and operations.
* Remove, install and test section equipment to accomplish equipment configurations as required to maintain 100% operational status of section equipment, to accomplish life- cycle equipment replacements, and to accomplish equipment upgrades and configuration changes.
* •Operate VTC equipment including powering up teleconferencing equipment, checking equipment for proper operation, setting audio levels, positioning camera functions, and performing secure or non-secure set-up. Assist Organization facilitators with conducting VTC, which may include conference preparation, monitoring VTC equipment and system performance, reporting equipment and network problems to appropriate parties and performing maintenance and repair. Perform operator level repairs of VTC equipment and repair or replace malfunctioning wiring, cabling and terminations associated with the equipment. Perform periodic maintenance on the VTC as specified by the manufacturer’s preventive and periodic maintenance specifications and the Government’s periodic maintenance schedule.
* •Develop SOPs for VTC scheduling, operation, and maintenance processes and procedures. Coordinate functional tests and scheduled VTCs with local and remote users, NEC, Defense Information Systems Global-Video Services (GVS), Defense Information Systems Network (DISN), and installation bridge operators. Conduct site surveys to validate equipment for all new requirements.
* •Perform VTC and A/V suite installation to include but not limited to televisions, speakers, Codec, Camera’s, and cabling. Provide expertise to Units on A/V requirements, sound management, noise conflict resolution etc.
* •Contractor may be required to procure cables, microphones, microphone stands, CODEC’s, conduit, etc. as required to meet the requirements in this PWS to setup and repair A/V and VTC equipment. Items purchased must be routed through the COR and approved by the KO and will be reimbursed on a separate supply CLIN per C.2.3.2 Purchases.

**C.4.4.1** Every contractor on this contract shall have the following qualifications before upon hiring:

•Cisco Video Network Specialist Certification (210-065 CIVND or current version),

•A SECRET security clearance is required upon hiring.

**C.4.5 Garrison above Baseline Help Desk Functions:** Primary place of performance is building 4, Fort Benning, GA. The Contractor shall:

* •Maintain the help desk ticketing system on SharePoint. Site shall be published to all Garrison users. Site shall function as the primary means for users to request IT support. Site shall be monitored daily and tickets routed appropriately. Contractor shall determine Baseline service requests and route those requests through AESD. Requests in AESD shall be created and tracked to completion.
* •Monitor continuously throughout duty hours. Assign tickets to appropriate techs. Track progress on resolution and keep the requestor informed of status.
* •The Contractor shall provide above-baseline Help Desk functions for all systems, software, and hardware associated with the Garrison functions, to include product support of Commercial of the Shelf (COTS) hardware and software, network support and repair services, printer support, computer imaging services, local touch labor troubleshooting, hand receipt functions, and cyclical replacements.
* •Assist with the design and maintenance of the portal environment and sites for the supported organization’s SharePoint presence on Government networks. Support day-to- day administration tasks such as group policy. Administer SharePoint top level sites and handle day-to-day user issues on SharePoint by recreating list and libraries, providing training and support to users.

**C.4.6 SharePoint / Azure Cloud Collaborative Tool Administration:** Develop and maintain the System Administrator SharePoint or Azure cloud collaborative tool site to include the collection and organization of data and metrics. Research various methods of collecting and tracking data and reporting in printable formats. Evaluating and improve existing processes and develop new processes where applicable. The contractor shall:

* Translate processes into SharePoint or Azure cloud collaborative tool; create and test configurations, folders, documents, calendars, other SharePoint objects, and scripts.
* •Provide Site Management/Site Collection Administration by performing end- user requirements gathering and definition support for web-portal based systems. Assist the Government in defining the solution approaches; identifying assumptions, constraints, risks and issues; defining users and system interfaces; improving portal design and functionality; and creating custom work flows. Assist the Government in developing the intended functional requirements, writing and managing the detail design, and reviewing and clarifying any questions or issues. Present the suggested solution to the Government for approval and implementation.
* •Assist with the design and maintenance of the portal environment and sites for the supported organization’s portal presence on Government networks. Support day-to- day administration tasks such as group policy.
* •Support the Government with IT requirements identification; data management and modeling; implementation of electronic business initiatives; and developing and executing concepts and programming objectives. Assist the Government in establishing requirements for portal services based on guidance/Garrison mission priorities. Support strategic planning for the design and use of collaboration tool. Provide planning, development, implementation and maintenance of portal programs and procedures to ensure availability of systems and data used by the Garrison and its supported organizations.
* •On a monthly frequency, the contractor shall provide Diagnostic technical support/help desk support reports indicating the number of support actions, the nature of the actions, measures of success/user satisfaction, identification of trouble areas, and recommended changes to processes or training requirements,
* •Resolve issues at supported organizations. Provide help desk services and technical support during normal duty hours.

**C.4.7 Senior Project Management Support:** The primary place of performance will be building 4, Fort Benning, Ga. The contractor shall: Provide PM support to the Fort Benning Garrison office tracking all aspects of the Garrison IT Services Contract.

* •Provide oversight for all activity conducted by contract staff.
* •Develop management plans and manage scope baseline.

**C.4.7.1** A SECRET security clearance is required upon hiring.

**C.4.7.2** Project Management Professional (PMP) certification from the Project Management Institute is required upon hiring.

# DELIVERABLES.

* + 1. **Performance Requirement Summary (PRS)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Required Service** | **Performance Threshold** | **Maximum Allowable Degree of Deviation for Requirement (Acceptable**  **Quality Level)** | **Method of Surveillance** | **Frequency of Inspection** |
| Provide IT Performance Metrics  (Para C.4) | Suspense date met – 98%.  Metrics collected will be complete and accurate – 95%. | 2% | 100%  Inspection | Quarterly |
| Database Management  Database Administration Services  (Para C.4) | Respond to Urgent Actions within 4 work hours – 98%  Resolve Urgent Actions within 1 work day – 100% | 2% | Periodic Inspection  Customer Complaints | Monthly |
|  | Respond to Routine Actions within 1 work day – 98% |  |  |  |
|  | Resolve Routine Actions within 2 working days – 95% |  |  |  |
|  |  |  |  |  |

* + 1. **IT Support Services Contract Deliverables**

**Title Frequency Delivered To**

Contract Status Report (C.4) Quarterly COR

IT Service Delivery reports (C.4) Weekly COR

Contract quality performance (C.4) Monthly COR Installation Status Report (ISR) (C.4) Quarterly COR

Management

Service Delivery performance (e.g., reliability, availability, etc.) by C4IM and Above Baseline IT Service category and function (C.4)

Monthly COR

Contractor’s Quality Control Program Within 15 calendar

days of performance start date

KO and COR

Database to track VTC suites inventory by unit, IP, location, POC, Site ID (C.4.4)

VTC Configuration Updates Report (C.4.4)

Summary report of available Garrison server space (C.4.7)

Monthly (Due NLT the 5th working day of the following month)

G-6 and COR

# Attachment 4 – Submission Instructions / Evaluation Criteria 4-A Evaluation Criteria

* + 1. Proposals shall evaluated based on the listed criteria:

**Technical Response**. Provide your technical approach to satisfying the requirements of the PWS. Discuss the unique aspects of the requirement (to include specific sections of the PWS) as applicable, and your approach to satisfying these requirements. Define the risks inherent in the requirement and/or your technical approach as well as your risk mitigation plan.

 **Staffing Plan:** Provide your plan to acquire and retain qualified personnel throughout the life of the contract. List personnel proposed by the sections of the PWS; include the labor categories and level-of-effort proposed per labor category for each of the PWS sections. Include the qualification requirements you will impose for each position proposed and discuss how the personnel proposed satisfy these qualification requirements. Discuss how the personnel proposed satisfy specific qualifications (to include security clearances) required by the PWS. Discuss the availability of the key personnel.

 **Specifically** discuss why you deem the experience to be relevant and of value to this requirement. Relevant experience of proposed personnel should be discussed under your staffing plan section. Discuss specific lessons learned or best practices developed that are relevant to this requirement.

 **Management Response.** Provide your management approach to satisfying the requirements of the PWS. In the event that subcontractors are proposed, discuss your communications and internal controls plan that will ensure satisfaction of the requirement. Discuss how you will update the Government and bring matters to the

attention of the Government. Discuss your performance, schedule and cost/price control plans. Discuss the need for and your approach to, adding team members at the task level to satisfy the unique requirements of this contract

 **Organization Structure:** Discuss your organization chart with a detailed explanation of the organization structure, including what the key positions are and what authority the individuals possess; what parts of the organization are responsible for managing and accomplishing what work; where decision making authority lies within the organization; and identify what work the prime, subcontractors or teaming partners are performing.

 **Personnel Qualification.** Discuss the qualifications of the proposed personnel.

 **Performance Information**. Provide past performance information regarding the quality of past performance on other relevant contracts or contracts.

# Price/Cost Response:

 Complete the proposed CLIN structure/schedule provided herein.

# 4 –B Instructions

1. The submission instructions are designed to provide general guidance for preparing responses as well as providing specific instructions on response organization, format, and content. Responders shall include all documents and information requested and shall be submitted in accordance with the instructions. The responder is cautioned to follow the instructions carefully, as the Government reserves the right to make an award based on initial responses received without discussion of such response.
2. Responders shall submit a response that is self-sufficient and responds directly to the requirements of the Request for Proposal (RFP). The response shall be clear, concise, and include adequate detail for effective evaluation. The response should not simply rephrase or restate the Government's requirements, but rather provide convincing rationale to address how the responder intends to meet the requirements of the RFP. The responses shall contain sufficient information to enable the Government to fully evaluate and determine the responder’s capability to comply with the requirements identified in the RFP. Responses that are overly verbose or include marketing material may distract from the evaluators ability to ascertain compliance with the RFP.
3. Responders shall submit a response that describes the procedures, processes, controls, etc. that are established for this RFP. The responders shall provide any assumptions upon which your approach/solution is based, and the rationale supporting the assumption (i.e., why do you believe the assumptions are valid). Express your best understanding of the ramification inherent in the contract. Discuss alternatives considered, risks involved, impact to the missions (both detriment, as well as efficiency), impacts from external sources, etc. Provide any other explanations or supporting data (matrix, charts, or other graphics) determined necessary for the Government to fully understand the responder’s methodology and approach.
4. In the event that travel is authorized in support of this contract, all travel charges shall be authorized in advance. Contractor travel charges will be invoiced in accordance with the current volume of the Government Joint Travel Regulations (JTR). Fee/profit on travel is not allowed.
5. The responder shall provide its response with a cover sheet that contains the company’s name, address and telephone number, name and title of the person authorized to sign and negotiate the contract, offer validation period of sixty (60) days, RFP number W911SF-18- G6 IT Support, and the original date of response. The original date shall be located in the upper right hand corner of the cover sheet.

# Basis of Award

FAR 52.217-5: Evaluation of Options

Except when it is determined in accordance with FAR 17.206 (b) not to be in the Government’s best interest, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

(End of provision)

This is a best value source selection conducted in accordance with the Federal Acquisition Regulation (FAR). Award will be made to a single offeror who is deemed responsible in accordance with the FAR, whose proposal conforms to the solicitation requirements and whose proposal, judged by an overall assessment of the evaluation criteria and other considerations specified in the solicitation, represents the Lowest Priced Technically Acceptable offer.

Trade-off between cost/price and non-cost/price factors is not permitted.

Award for all of the Work. The Government intends to award one (1) contract as a Result of this solicitation. Offers received for less than the stated number of items listed in the Bid Schedule will be considered ineligible for award. The Government intends to evaluate proposals and award without discussions with offerors The Government reserves the right to conduct discussions if the Contracting Officer determines them to be necessary.

# Evaluation Criteria

* + 1. The Government reserves the right to evaluate the lowest priced proposal first, and if it is acceptable, award to that offeror. In the event that the lowest price proposal is not acceptable, the second lowest proposal will be evaluated, and so on. The Evaluation Criteria will consist of factors, sub factors and elements. The proposals will be evaluated using four evaluation factors.

Factor 1 & 2: Technical Capability

Sub factor 1: Management/Staffing Approach

Sub factor 2: Technical Ability

Factor 3: Past Performance

Factor 4: Price

* + 1. Factors 1 & 2 - Technical Capability

The technical factor will receive one of the adjectival ratings defined below. The sub factor ratings will be used to determine than overall rating for the factor. Any unacceptable rating in a sub factor will result in an unacceptable rating for Technical capability.

|  |  |
| --- | --- |
| Technical Ratings | |
| Rating | Description |
| Acceptable | Proposal clearly meets the requirements of the solicitation |
| Unacceptable | Proposal does not clearly meet the minimum requirements of the solicitation |

a. Factor 1: Technical Acceptability, Subfactor 1: Staffing/Management Approach

The offeror’s proposal must demonstrate the capability to provide a Staffing/Management approach response which shall contain sufficient quantitative details (without reference to cost or price) to permit a complete and accurate evaluation. From the PWS, the proposal must include and address:

-C.3.4 Contractor Accountability task (C.3.19 Quality Control, C.3.23 Key Personnel, C.3.24 Government Driver’s License, C.3.27 Applicable Documents)

-Internal and External communication and performance schedules.

b. Factor 2: Technical Acceptability, Subfactor 2: Technical Ability

The offeror’s proposal must demonstrate the capability to provide Technical Ability to complete all tasks in the PWS, which shall contain sufficient quantitative details (without reference to cost or price) to permit a complete and accurate evaluation. From the PWS, the proposal must include and address:

-C.4 Specific Tasks (C.4.1. Garrison IMO Support, C.4.2 Above Baseline System Administration, C.4.3 Development of New IT Solutions, C.4.4. G-6 Audio/Visual Teleconferencing Support, C.4.5 Garrison Above Baseline Help Desk Functions, C.4.6 SharePoint/Azure Cloud Collaborative Tool Administration, C.4.7 Senior Project Management Support).

* + 1. Factor 3 – Past Performance

The offeror’s proposal shall provide documentation outlining the offeror’s past performance with contracts, as a prime or subcontractor, which is the same or similar in nature, size, and complexity to the services being procured under this solicitation. The submittal shall include rationale supporting your assertion of relevance and how it was determined that the work performed previously was the same or similar in nature, size, and complexity to the work specified by this solicitation. The Past Performance evaluation will be accomplished by reviewing aspects of an Offeror's recent and relevant Past Performance, focusing on and targeting performance which is relevant to the effort as it relates to the services being procured under this solicitation.

* + 1. Factor 4 - Price

Price will not be scored or rated. Evaluation of price will be performed using one or more price analysis techniques in FAR 15.404-1 (b). Through these techniques the Government will determine whether prices are reasonable, complete and balanced. The responder’s price submission will be evaluated considering the response to the contract and the pricing matrix of the TO. The techniques and procedures described under FAR Part 15.404 will be the primary means of assessing price submission reasonableness. To be viable for award, responder’s price must be determined fair and reasonable. The Government price team will evaluate responder’s price submission for reasonableness based on the following:

1. Reasonableness will be determined by comparing the responder’s total cost proposed to the total costs proposed by the other responders. Additionally, total proposed prices may be compared to the Independent Government Estimate (IGE) to determine the reasonableness of price.
2. The responder’s price submission shall represent the responder's best efforts to respond to the RFP. Any inconsistency between promised performance and price shall be explained in the submission. For example, if unique, innovative approaches are the basis for an unusually low price, the nature of these approaches and their impact on price shall be explained. If a responder proposes to absorb a portion of price, the responder must also explain the impact on the estimated price. Any significant inconsistency, left unexplained, may raise a fundamental question of the responder's understanding of the nature and scope of the work required in the contract, and of the responder's ability to perform the tasks within the fiscal constraints thereof, and may be cause for rejection of the submission. The burden of proof for price credibility rests with the responder.
3. As part of price As part of price evaluation, the Government will evaluate its options to extend services (see FAR Clause 52.217-8) by adding one – half of the offeror’s final option period price to the offeror’s total price. Thus, the offeror’s total price for the purpose of evaluation will include base period, all four option periods (FAR 52.217-9), and one –half the fourth option. Offerors are not required to enter a price for the six-month period immediately following the end of the fourth option year (FAR 52.217-8).