PERFORMANCE WORK STATEMENT (PWS)

for

Cyber Capability Development Integration Directorate,
Future Concepts Center, Army Futures Command

Cyberspace, Electronic Warfare, Signal, and Information Related Capabilities Modernization Support to the Cyber Center of Excellence

Indefinite Delivery, Indefinite Quantity (ID/IQ)

Rev: Oct 23, 2020

HEADQUARTERS
Cyber Capability Development Integration Directorate
FORT GORDON, GA 30905-5000

Part 1
General Information

1. GENERAL: This is a non-personal services contract to provide the US Army Cyber Capability Development Integration Directorate (CDID) with support services in the following capability areas:

1. Operations, Administration, and Program Management
2. Experimentation and Evaluation
3. Concept Development
4. Requirements Development
5. Analytical Support
6. Force Modernization Proponent Integration
    - Capability Management
    - Force Design
    - Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) Integration
    - Threat and Operational Environment (OE)

The Government will not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the contractor who, in turn is responsible to the Government.

1.1 Description of Services/Introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Capability Modernization as defined in this Performance Work Statement (PWS) except for those items specified as Government furnished property and services. The contractor shall perform to the standards in this PWS, Task Order PWS and Performance Requirements Summary (PRS).

1.2 Background: In support of Army Futures Command, Futures & Concepts Center, and General Support to the Cyber Center of Excellence the Force Modernization Proponent for Cyberspace Operations, Signal/Communications, and Electronic Warfare, Cyber CDID develops, evaluates, integrates, and communicates concepts, requirements, and solutions across DOTMLPF, Warfighting functions, and formations to improve the Army and ensure the combat effectiveness of the future force.

1.3 Objectives: This multiple award indefinite delivery, indefinite quantity (MA IDIQ) will require vendors to research, conceptualize, produce, develop, communicate, analyze, engineer, evaluate, review, and inform products required to develop capability requirements for the modernization Signal/Communications, Cyberspace Operations, Electronic Warfare, and Information Related capabilities.

1.4 Scope: As an independent contractor and not as an agent of the Government, the contractor(s) shall provide all labor, material and services, except as specified to be furnished by the Government, necessary to perform the types of tasks specified herein. The specific work to be performed under this contract shall be initiated through the issuance of individual task orders in accordance with the solicitation. Individual task order PWSs shall include definitive task requirements, deliverables, and special requirements. Performance under each task order shall follow the Schedule for submission of deliverables along with In-Progress Reviews (IPR) stated therein. Specific requirements under this contract will be identified at the task order level.

1.4.1 The Government and the contractor understand and agree that the work described in this contract and task orders issued under the contract is a "Non-personal Services Contract" as defined in FAR Part 37.101. Therefore, it is further understood and agreed that the contractor and/or sub-contractors and/or contractor/sub-contractor employees:

(1). Shall perform the services described herein as independent contractors, not as employees of the Government.
(2). Shall NOT be placed in a position where they are under the supervision, direction or evaluation of a federal employee, military or civilian, but shall, pursuant to the Government's right to inspect, accept or reject work, comply with such general direction of the Contracting Officer or the duly appointed representative of the Contracting Officer as is necessary to ensure completion of the contract objectives.
(3). Shall NOT be placed in a position of command, supervision administration or control over DA military, civilian personnel, or personnel of other contractors, or become part of the Government organization.
(4). Shall perform services on contract/task order and does not create an employer-employee relationship, the entitlements and benefits applicable to such relationships do NOT apply.

1.5 Ordering Period: The period of performance shall be for a five (5) year ordering period beginning June 21, 2021.

1.6 General Information

1.6.1 Quality Control: The contractor is responsible for the quality of the products/services delivered under the terms and conditions of this contract and all task orders to this contract. The contractor shall develop and maintain an effective Quality Control Plan/Program (QCP) that is acceptable to the Government. The plan shall ensure all products/services required by this master indefinite delivery indefinite quantity (ID/IQ) contract and all task orders are delivered in accordance with all the requirements of this PWS as well as the associated task order PWSs. The contractor’s QCP shall implement procedures

which identify, prevent, and ensure non-recurrence of defective services. The QCP shall be delivered to the Government within thirty (30) days of contract performance start and the Government will have ten (10) working days to review and accept or send the plan back for revision. In the event revisions are required the contractor shall make the appropriate revisions and return the revised QCP to the Government within five (5) working days of receipt of notification to revise. After acceptance of the QCP by the Contracting Officer any future proposed revisions must be submitted to the Contracting Officer's Representative (COR) and Contracting Officer for approval.

1.6.2 Quality Assurance: The Government will evaluate the contractor's performance under this contract in accordance with the MA IDIQ and individual TO Quality Assurance Surveillance Plans (QASP). The QASP is a Government only document primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. The QASP defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.6.3 Recognized Holidays: The contractor shall not perform work on days when legal public holidays are observed by federal employees whose basic workweek is Monday through Friday unless an exception is specified in the individual task order. When a legal public holiday occurs on a Saturday or Sunday, the holiday is observed on the preceding Friday or following Monday, respectively. Legal public holidays are established in 5 U.S.C §6103 and include:

New Year's Day	1st day of January
Martin Luther King Jr.'s Birthday	3rd Monday of January
Presidents' Day	3rd Monday of February
Memorial Day	Last Monday of May
Independence Day	4th day of July
Labor Day	1st Monday of September
Columbus Day	2nd Monday of October
Veterans Day	11th day of November
Thanksgiving Day	4th Thursday of November
Christmas Day	25th day of December

1.6.4 Hours of Operation: The contractor is responsible for conducting business, between the hours of 0800 – 1700 Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The contractor must at all times 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.

1.6.5 Place of Performance: The place of performance shall be specified in each task order. Primary places of performance is the US Army Cyber Center of

Excellence (CCoE), Fort Gordon, Georgia, and specified Government facilities.. If place of performance changes, a modification to the task order will be issued by the Contracting Officer. Place of duty will be specified in the event of contractor travel.

1.6.6 Type of Contract: The Government will award a multiple award task order contract (MATOC).

1.6.7 Security Requirements: Due to the sensitive nature of working with Warfighter requirements, known system vulnerabilities, and mission gaps, contractor employees performing on this contract and all task orders must be U.S. citizens and have at a minimum a SECRET clearance on work performance start date. The highest security level involved in this contract is TOP SECRET with access to Secure Compartmentalized Information (SCI), depending on task order requirements. Security requirements will be stated in each task order. The contractor shall acquire the clearances and all contractor employees shall maintain the minimum required security clearance throughout the life of the supported task order. The security requirements are in accordance with the Attachment 2 , DD 254.

1.6.7.1 The contractor shall ensure that classified data is controlled, protected, and safeguarded in accordance with AR 380-5 and current Army and DOD policy. Information classified up to TOP SECRET shall be accessed and stored in Government spaces only. The contractor shall agree that any data furnished by the Government to the contractor shall be used only for performance under this PWS and task order PWSs, and all copies of such data shall be returned to the Government upon completion of this effort. Compliance with DD 254, Department of Defense Contract Security Classifications Specifications, is required.

1.6.7.2 The contractor Facility Security Officer (FSO) shall ensure there is a procedure for all terminated employees to out process the installation.

1.6.7.3 PHYSICAL Security: The contractor shall be responsible for safeguarding all Government equipment, information and property provided for contractor use in accordance with Army Regulation (AR) 190-13 (27 Aug 19) and AR 190-51 (27Jun 19). At the close of each work period, Government facilities, equipment, and materials shall be secured.

1.6.7.4 Key/Token Control: The contractor shall establish and implement methods in accordance with AR 190-11 (17 Jan 19) to make 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 and tokens. No keys issued to the contractor by the Government will 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 and Key Control Officer/Security Officer.

1.6.7.4.1. In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon direction of the Contracting Officer's Representative or 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.

1.6.7.4.2. The contractor shall prohibit the use of Government issued keys/key cards to 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's Representative.

1.6.7.5 Lock Combinations/Access Control Codes. The contractor shall establish and implement methods of ensuring that all lock combinations/access control codes are not revealed to unauthorized persons. The contractor shall ensure that lock combinations/access control codes are changed when personnel having access to the combinations/access control codes no longer have a need to know or are no longer employees of the company. These procedures shall be included in the contractor's Quality Control Plan.

1.6.7.6 The contractor shall adhere to local Operations Security (OPSEC) policies and procedures of the Government requiring activity. When conducting contractor travel in support of this work effort, the contractor shall also adhere to any OPSEC policies and procedures in effect at TDY locations.

1.6.7.7 Installation Access: All contractor employees, including subcontractors, shall comply with applicable installation and facility access security policies and procedures at all work and TDY locations. All contractors and subcontractors will be issued a Common Access Card (CAC) or an Installation Pass issued through the Automated Installation entry (AIE) Security System to access the installation. The Fort Gordon military installation is a limited access post. Unscheduled gate closures by the military police may occur at any time. In accordance with AR 525-13 (3 Dec 2019), paragraph 5-19, all prospective contractors shall undergo a verification process by the installation Provost Marshal Office, Director of Emergency Services to determine the trustworthiness and suitability prior to being granted access to federal property. This will be accomplished using the National

Crime Information Center (NCIC) Interstate Identification Index (III). This is the minimum baseline background check for entrance onto Army Installations for non-CAC holders to include entrance of visitors (Ref AR 190-13 (27 Jun 2019), paragraph 8-2). All personnel entering or exiting the installation may experience a delay due to vehicle inspections, registration checks, verification of seat belt use, etc. All vehicles and personnel are subject to search and seizure. The search and seizure provisions shall apply to contractor personnel while within Fort Gordon's area of jurisdiction. Contractor personnel shall comply with all entry control requirements and security policies/procedures in effect. Security procedures may change without notice.

1.6.7.8 SIPRNET access is required to perform tasks under this contract. Each TO PWS will identify tasks/contract employees that are required to have SIPRNET access. The contractor is not authorized to access, download or further disseminate any classified information from SIPRNET which is outside the scope of the defined contract requirements unless specifically authorized in writing by the Government Program Manager and the KO. The contractor must complete and forward to the COR, a SIPRNET Access Request Form for approval by the Requiring Activity SIPRNET Information Assurance Manager (IAM) prior to receiving access. NOTE: A NATO Awareness brief and acknowledgement is required for all personnel prior to access to the SIPRNET. Since the SIPRNET contains NATO information, a NATO Awareness briefing informing personnel how to protect NATO information is mandatory for everyone who requires access to the SIPRNET. A written acknowledgment shall be maintained by the COR.

1.6.7.9 Cybersecurity (formerly Information Assurance (IA)/Information Technology (IT)) Training. All contractor employees and associated subcontractors must complete the DoD Cyber Awareness Challenge Training (https://ia.signal.army.mil/DoDIAA) upon task order award and annually thereafter. Certificates of successful completion, for both initial awareness training and annual refresher training shall be provided to the COR via the Army Training and Certification Tracking System (ATCTS). All contractor employees will successfully complete all required IA training as specified in AR 25-2 and as directed by the Government. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01 (23 Apr 2015), DoD 8570.01-M (10 Nov 2015), DoDD 8140.01 (31 Jul 2017), and AR 25-2 (4 Apr 2019).

1.6.7.10 Cybersecurity (formerly Information Assurance (IA)/Information Technology (IT)) Certification. Per DoD 8570.01-M, / DoD 8140 DFARS 252.239.7001, and AR 25-2, the contractor employees' supporting IA/IT functions shall be appropriately certified upon task order award. The baseline certification must be completed as stipulated in DoD 8570.01-M / DoD 8140.

1.6.7.11 Annual Security Refresher Training. All contractor employees, including subcontractors, assigned to this contract shall complete the online Annual

Security Refresher Training located on the Army Learning Management System (ALMS) site. Log into AKO, “Self Service”, “My Training”, “ALMS”, “Go to Mandatory Training”. Training must be completed within 30 days of task order award. The contractor shall submit certificate of completion for each affected contractor employee and subcontractor employee to the COR and unit/activity security manager. (Ref ALARACT 207/2013, DTG 291848Z Aug 13, Subj: Army Wide Rollout and Requirement for Standardized Computer Web-Based Security Training on the ALMS website.

1.6.7.12 Anti-Terrorism (AT) Level I Training. All contractor employees, including subcontractors, assigned to this contract shall receive an initial Antiterrorism Level I Brief by a certified ATO Level II Officer within 30 days of task order award. (Monthly briefings will be offered by the Garrison Antiterrorism Officer.) Annual refresher Antiterrorism Level I Training shall be completed on-line at https://atlevel1.dtic.mil/at/ or they may attend the monthly training offered by the Garrison ATO. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR and unit/activity security manager. (Ref Department of the Army, US Army Contracting Agency, SFCA-CO, 5 Sep 2007, subject: Incorporation of Measures into the Contracting Process and AR 525-13, Antiterrorism, 3 Dec 2019). Note: Contractor personnel shall receive an AOR briefing when traveling OCONUS on TDY. Briefing must be provided by a certified ATO Level II Officer within 7 working days prior to TDY departure outside the 50 United States, its territories, and possessions. This is separate from the normal annual AT Level I training requirement. (Ref AR 525-13)

1.6.7.13 iWATCH: All contractor employees, including subcontractors, assigned to this contract shall receive a brief on the local iWATCH program (provided in conjunction with the AT Level I Training). This 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 days of task order award and annual refresher training with the results reported to the COR.

1.6.7.14 Operation Security (OPSEC) Training. All contractor employees, including subcontractors, assigned to this contract shall complete Level I OPSEC training within 30 days of task order award and then annually thereafter. Initial Level 1 OPSEC training will be conducted monthly by the Garrison OPSEC Officer or a Level II certified OPSEC Officer. Annual refresher training shall be completed on-line at http://cdsetrain.dtic.mil/opsec/index/htm. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR and unit/activity security manager. (Ref AR 530-1, Operations Security). The contractor shall adhere to local OPSEC policies and procedures of the Government requiring activity. When in a TDY status in support of this work effort, the contractor shall also adhere to any OPSEC policies and procedures in effect at TDY locations.

1.6.7.15 Threat Awareness and Reporting Program (TARP) Training. All contractor employees, including subcontractors, assigned to this contract shall complete TARP training within 30 days of task order award and then annually thereafter. TARP training will be conducted monthly by the 902nd MI Group. The COR will ensure contractors are notified of available training. Completion of training shall be reported to the COR and the unit/activity security manager. (Ref AR 381-12).

1.6.7.16 Derivative Classification Training: Within 30 days of task order award all contractor employees assigned to this contract shall complete Derivative Classification Training, in accordance with Volume 2 of DoD Manual 5200.01, “DoD information Security Program.” Derivative classification is the act of reproducing, extracting, summarizing, incorporating, paraphrasing, restating, or generating, in a new form, information already classified and marking the newly developed material consistent with the classification and marking applied to the source information. Contractor employees shall have the Initial Derivative Classification Course (course number IF103.16) at from the Center for Development of Security Excellence (CDSE) online at https://cdse.usalearning.gov. After the initial course, contractors may take the refresher course, course number IF109.16, to fulfill this annual requirement. Contractor employees with TS/SCI clearances shall take CDSE course SCI100.16, Sensitive Compartmented Information Familiarization (SCI) Refresher Training annually.

1.6.8 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 FAR 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 shall apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues.

1.6.9 Contracting Officer Representative (COR): The COR will be officially appointed to the contractor, in writing, by the Contracting Officer. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the contractor concerning technical aspects of the contract; 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 appointment 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.

1.6.10 Key Personnel: The contractor shall provide program managers/site-leads as specified in individual task orders who shall be responsible for the performance of the work.

1.6.11 Special Qualifications: See appendix A, Specific Qualification Requirement.

1.6.12 Identification of contractor Employees: In accordance with FAR 37.114 contract employees shall identify themselves as a contractor at all times while on the job, e.g., in the workplace, when attending meetings, in email, when answering Government telephones, or when making phone calls.

1.6.12.1 Common Access (CAC) Badges: Each Contractor employee will be required to obtain a CAC issued by the Government. Each Contractor employee's name social security number, date of birth and email address will entered into a database (by the COR called the Contractor Verification System (CVS). CVS is automated system to allow Contractors personal information to be verified when applying for a new or renewal Government identification card referred to as the CAC. Once the Contractor employee's information is registered, the COR will electronically forward the form to the contractor. Each contractor employee is required to electronically fill out the CAC request form. Once the form is properly filled out, the COR will verify that they authorized and required to have a CAC. The contractor employees will be directed to go to the designed in processing facility and obtain the CAC. Should an employee leave prior to the contractor expiration, the contractor is responsible for ensuring the immediately be delivered to the COR for cancellation upon the release of any employee. Failure, inability, or delay in obtaining the CAC does not relieve the contractor from performing under terms of the contractor. Contractor employees must maintain possession of issued Common Access Cards at all times when performing work under this contract.

1.6.12.2 Display of CAC Badges: When not in use as authentication, contractor personnel shall wear the CAC as a badge when performing work under this contract to include attending government meetings and conferences. Unless otherwise specified in the contract, each contract personnel shall wear the CAC

badge in a conspicuous place on the front of exterior clothing and above the waist except when safety or health reasons prohibit such placement.

1.6.12.3 Answering Telephones. Contractor personnel shall identify themselves as contract employees when answering and making calls on Government telephones.

1.6.12.4 Utilizing Electronic Mail. When contractor personnel send e-mail messages to Government personnel while performing on this contract, the contractor personnel e-mail addresses shall include the company name together with the person's name (ex: John Smith, contractor, ABC Company). When any contractor personnel require access to a Government computer, the contractor personnel shall be required to obtain a CAC. To do so, the contractor personnel shall request a CAC Card through the COR, and shall complete an automated DD Form 1172-2 application through the) Trusted Agent Sponsorship System. The Government issued CAC is the property of the U.S. Government and shall be returned to the COR upon expiration of the contract, replacement or termination of the contract employee. (CAC card shall be turned in to the COR on contractor's last day of employment.) Unauthorized possession of the CAC can be prosecuted criminally under section 701, title 18, United States Code. All contractor employees shall conduct official communication using Government-owned or provided e-mail, networks, websites, systems, and devices. The use of commercial ISP e-mail accounts or personal e-mail accounts to conduct official communication is prohibited. Remote access / telework technology may be leveraged to ensure compliance with these requirements. Contractor employees are prohibited from using Army-assigned, AKO, and other official e-mail addresses for unofficial business affiliations. Personnel shall not provide official e-mail addresses to businesses, affiliated organizations, or online retailers; unless those entities are known by personnel to be legitimately engaging in official business.

1.6.13 Contractor Travel: The contractor shall perform official contract travel to CONUS and OCONUS locations as required by task orders under this contract. Additionally, the contractor shall be able to maintain any required host nation authority, licenses, or other permission to operate within the country.

1.6.13.1 When the contractor is required to travel within the CONUS and OCONUS to support tasks and requirements described within this PWS and/or a task order PWS, Significant Activity (SIGACT) reports shall be completed and submitted to the Government in accordance with corresponding deliverable.

1.6.13.2 The contractor shall provide a cost estimate to the COR and obtain the COR's approval prior to travel. Travel shall not commence prior to obtaining the COR's approval. Reimbursement for travel will be IAW the Federal Acquisition Regulation (FAR) 31.205-46. The contractor shall submit invoices for reimbursement citing the appropriate contract line item (CLIN). All supporting

documentation for travel shall be legible, error free, and shall state the exact amount the Government owes the vendor.

1.6.13.3 Travel costs shall be deemed reasonable and allowable only IAW FAR 31.205-46. Travel is designated as a Cost Reimbursable expense. Invoices shall have complete supporting documentation of costs attached with an itemization of costs by trip/personnel. The contractor will be paid incurred costs and Per Diem and travel in accordance with Joint Travel Regulations. The contractor must provide proof of the actual amount paid to the employee. Unsubstantiated costs will not be allowed. Maximum use shall be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours. All necessary travel meeting the above criteria shall be approved in advance by the COR or other designated Government representative. Explicit written approval of the COR or other designated Government representative is required for all travel. Exceptions to these guidelines shall be approved in advance by the Contracting Officer or his/her Designee. The COR/other designated Government representative will give the contractor a minimum of 5 workday notice of a scheduled trip. The Government representative may change a scheduled trip by giving 2-days written notice, provided no costs have been incurred by the contractor. The contractor shall be required to travel when determined necessary by the Government. The contractor shall notify the COR before chargeable costs exceed the “not to exceed” funding provided on the order.

1.6.13.4 The contractor shall use only the minimum number of travelers and rental vehicles needed to accomplish the mission. Travel will be by the most economical carrier and scheduled during normal business hours, whenever possible. No Cost changes to the travel schedule may be made by the designated Government representative up to the point of departure.

1.6.13.5 Since the actual number of days for each travel cannot be pre-determined the contractor shall be required to comply with AR 715-9, Operational Contract Support Planning and Management, dated 20 June 2011. This regulation addresses how contract employees in an Area of operations are supported by a unit and the relationship to the unit. The only time this would apply is when a contractor is sent OCONUS to work within a unit.

1.6.13.6 Subsequently, Non-Unit Related Personnel (NRP) deploying for less than 30 days will not process through CONUS Replacement Component (CRC) and may receive an exception to processing based upon individual case-by-case requirements as coordinated with the designated CRC. Pre-approved travel and material expenses may be billed back to the Government under this contract.

1.6.13.7 Other Direct Costs. ODC’s are costs not previously identified as a direct material cost or direct labor cost, that can be identified specifically with a final cost objective and are only authorized to the extent that they are necessary for

performance of individual TOs under this contract. Labor is not permitted to be proposed as an ODC. Allowable other direct costs will be determined by the Contracting Officer at the TO level and may be added to individual TOs as a separate CLIN on a cost reimbursement basis only.

1.6.14 Data Rights: The Government’s rights in non-commercial technical data and software deliverables shall be governed by DFARS 252.227-7013 and DFARS 252.227-7014, respectively. The Government's rights in commercial technical data deliverables shall be governed by DFARS 252.227-7015. All non-commercial technical data and software deliverables shall be properly marked in accordance with the marking requirements set forth in DFARS 252.227-7013(f) and DFARS 252.227-7014(f), respectively. Technical data and software deliverables with non-conforming restrictive markings shall be rejected and corrected by the Contractor at the Contractor's expense, in accordance with DFARS 252.227-7013(h)(2) and DFARS 252.227-7014(h)(2), respectively.

1.6.15 Organizational Conflict of Interest:

Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor’s mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary

including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

a. Purpose. The primary purpose of this clause is to aid in ensuring that:

(1) The contractor does not obtain an unfair competitive advantage by establishing the ground rules for a future competition;

(2) The contractor's objectivity and judgment are not biased because of its present or future interests (financial, contractual, organizational, or otherwise) which relate to work performed under this contract; and

(3) The contractor does not obtain an unfair competitive advantage by virtue of its access to non-public or proprietary information belonging to others.

b. Definitions.

(1) The term “contractor” herein used means: (a) the organization (hereinafter referred to as "it" or "its") entering into this agreement with the Government; (b) all business organizations with which it may merge, join or affiliate now or in the future and in any manner whatsoever, or which hold or may obtain, by purchase or otherwise, direct or indirect control of it; (c) its parent organization if any and any of its present or future subsidiaries, associates, affiliates, or holding companies, and; (d) any organization or enterprise over which it has direct or indirect control now or in the future.
(2) The term "proprietary information" for purposes of this clause means any information considered so valuable by its owners that it is held secret by them and their licensees. Information furnished voluntarily by the owner without limitations on its use, or which is available without restrictions from other sources, is not considered proprietary.

c. Organizational Conflicts of Interest Examples. The following examples illustrate situations in which organizational conflicts of interest may arise. These examples are not all inclusive.

(1) Biased Ground Rules. This type of conflict may arise in situations where a company sets the ground rules for a future competition. For example, when a contractor develops requirements then competes to provide products or services to satisfy those requirements, thus obtaining a competitive advantage.

(2) Impaired Objectivity. This type of conflict may exist where a contractor’s obligations under a contract require objectivity, but another role of the contractor casts doubt on its ability to be truly objective. An example of this type of conflict is

where a contractor's work under one contract entails evaluating itself, its affiliates, or its competitors under a separate contract.

(3) Unequal Access to Information. This type of conflict may arise when a contractor has access to nonpublic or proprietary information as part of its performance under a contract that gives it an unfair advantage in a competition for a later contract.

d. General Constraints. The provisions of FAR Subpart 9.5, Organizational and Consultant Conflicts of Interest, concerning organizational conflicts of interest govern this contract. Potential conflicts may exist in accordance with FAR 9.505-1, Providing Systems Engineering and Technical Direction, through 9.505-4, Obtaining Access to Proprietary Information. In this regard, the contractor is responsible for identifying any actual or potential organizational conflicts of interest to the Contracting Officer that arise as the result of performance under this contract. To avoid or mitigate a potential conflict related to performance under this contract, the Contracting Officer will impose appropriate constraints such as the constraints discussed below. Since it is impossible to foresee all of the circumstances that might give rise to organizational conflicts of interest, the constraints discussed below are not all inclusive and the Contracting Officer may impose constraints other than, or in addition to, the constraints listed below.

(1) The contractor agrees that if it provides, under a contract or task order or delivery order, systems engineering and technical guidance for systems and programs, but does not have overall contractual responsibility, it will not be allowed to be awarded a contract or task or delivery order to supply the system or any of its major components or be a subcontractor or consultant to a supplier of the system or any of its major components. (FAR 9.505-1).

(2) The contractor agrees that if it prepares complete specifications for non-developmental items or assists in the preparation of work statements for a system or services under a contract or task order or delivery order, it will not be allowed to furnish these items, either as a prime contractor, a subcontractor or as a consultant. (FAR 9.505-2).

(3) The contractor agrees that it will neither evaluate nor advise the Government with regard to its own products or activities. The contractor will objectively evaluate or advise the Government concerning products or activities of any prospective competitors. (FAR 9.505-3).

(4) The contractor agrees that if it gains access to proprietary information of other companies, it will exercise diligent effort to protect such proprietary information from unauthorized use or disclosure. (FAR 9.505-4). In addition, the contractor agrees to protect the proprietary information of other organizations disclosed to the contractor during performance of this contract with the same caution that a reasonably prudent contractor would use to safeguard highly valuable property.

The contractor also agrees that if it gains access to the proprietary information of other companies it will enter into written agreements with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and to refrain from using the information for any purpose other than that for which it was furnished. The contractor shall provide copies of such agreements to the Contracting Officer.

(5) If the contractor, in the performance of this contract, obtains access to plans, policies, reports, studies, financial plans, data or other information of any nature which has not been released or otherwise made available to the public, the contractor agrees that without prior written approval of the Contracting Officer, it shall not: (a) use such information for any private purpose unless the information has been released or otherwise made available to the public, or (b) release such information unless release is otherwise authorized under the contract or such information has previously been released or otherwise made available to the public by the Government.

e. Non-Disclosure Agreements. The contractor shall obtain from each employee who has access to proprietary information under this contract, a written agreement which shall in substance provide that such employee shall not, during his/her employment by the contractor or thereafter, disclose to others or use for their benefit, proprietary information received in connection with the work under this contract. The contractor will educate its employees regarding the restrictions imposed by FAR 9.505-4 so that they will not use or disclose proprietary information or data generated or acquired in the performance of this contract except as provided herein.

f. Training. The contractor shall effectively educate its employees, through formal training, company policy, information directives and procedures, in an awareness of the legal provisions of FAR Subpart 9.5 and its underlying policy and principles so that each employee will know and understand the provisions of that Subpart and the absolute necessity of safeguarding information from anyone other than the contractor's employees who have a need to know, and the U.S. Government.

g. Subcontracts. The contractor agrees that it will include the provisions in paragraphs d., e., and f. above and this paragraph in consulting agreements, teaming agreements, and subcontracts of all tiers which involve access to information or the performance of services described in paragraph d. above. The use of this clause in such agreements shall be read by substituting the word "consultant" or "subcontractor" for the word "contractor" whenever the latter appears.

h. Additional Constraints. If this contract provides for the issuance of task or delivery orders, such orders may impose additional requirements and restrictions relating to this clause to include the requirement for the contractor and its subcontractors and employees to furnish the Government with written non-

disclosure agreements or statements of no conflict of interest. With regard to any proposal submitted by the contractor in response to a Request for Task or Delivery Order Proposal, by submitting its proposal the contractor represents that it has disclosed to the Contracting Officer, prior to the issuance of the task or delivery order, all facts relevant to the existence or potential existence of organizational conflict of interest as that term is used in FAR Subpart 9.5.

i. Conflicts Involving Future Procurements. The award of this contract, task or delivery orders issued under this contract, Government taskings, or acquiescence in the contractor's performance of services hereunder shall not constitute or be interpreted as a determination that the contractor is eligible to participate in future procurements, developmental efforts, implementation efforts, or related activities. Only the Contracting Officers for such efforts, applying the rules, principles, and procedures of FAR Subpart 9.5 have the authority to determine whether a conflict exists in connection with such procurements.

j. Representations and Disclosures.

(1) The contractor represents that it has disclosed to the Contracting Officer, prior to award of this contract, all facts relevant to the existence or potential existence of organizational conflict of interest as that term is used in FAR Subpart 9.5.

(2) The contractor represents that if it discovers an organizational conflict of interest or potential conflict of interest after award of this contract, a prompt and full disclosure shall be made in writing to the Contracting Officer. This disclosure shall include a description of the action the contractor has taken or proposes to take in order to avoid or mitigate such conflict.

k. Remedies and Waiver.

(1) For breach of any of the above restrictions or for non-disclosure or misrepresentation of any relevant facts required to be disclosed concerning this contract, the Government may terminate this contract for default, disqualify the contractor for subsequent related contractual efforts, and pursue such other remedies as may be permitted by law or this contract. If, however, in compliance with this clause, the contractor discovers and promptly reports an organizational conflict of interest (or the potential thereof) subsequent to contract award, the Contracting Officer may terminate this Contract or any task or delivery order issued under this Contract for convenience if such termination is deemed to be in the best interest of the Government.

(2) The parties recognize that this clause has potential effects which will survive the performance of this contract and that it is impossible to foresee each circumstance to which it might be applied in the future. Accordingly, the contractor may at any time seek a waiver from the cognizant Contracting Officer

by submitting a full written description of the requested waiver and the reasons in support thereof. (FAR 9.503).

1.6.15.1 Disclosure of Activities or Information. The contractor shall not divulge or cause to be divulged any information accessed and obtained during the course of performing tasks to other contractor staff or anyone outside the Government. In addition to any organizational conflict of interest provision, contractor employees assigned may be required, prior to beginning work, to sign a non-disclosure statement for the Government agreeing not to share any information or data with other contractor personnel not assigned to the project or, if assigned to the project, who has not signed a non-disclosure statement. Signed nondisclosure statements shall be furnished to the COR prior to contract performance. Final authorship and copyright of any deliverables shall reside with the Government to include all training materials developed under this contract. The contractor shall identify any organizational conflict of interest clauses they or their subcontractors are subject to, current or within three years of federal Government contract services, by providing, with their offer, a copy of the clause, a description of the contract services performed, a contract number, a Governmental point of contact, and a phone number for that point of contact. The contractor shall refer outside requests for information to the Government. The contractor shall obtain prior permission from Fort Gordon, GA Public Affairs Office (PAO) and the COR for the use of any Army Futures Command, Futures & Concepts Center, Fort Gordon, GA, Cyber Center of Excellence, or Cyber CDID logos, and photos in any advertisements or announcements.

1.6.16 PHASE IN /PHASE OUT PERIOD: Any requirements for Phase-In/Phase-Out will be identified and accomplished at the TO level.

PART 2
DEFINITIONS & ACRONYMS

2. DEFINITIONS AND ACRONYMS:

2.1. DEFINITIONS:

2.1.1. CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

2.1.2. CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the Government. Note: The only individual who can legally bind the Government.

2.1.3. CONTRACT ADMINISTRATOR. The official Government representative delegated authority by the Contracting Officer to administer a contract. This individual is normally a member of the appropriate Contracting/Procurement career field and advises on all technical contractual matters.

2.1.4. CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the Contracting Officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.5. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the PWS.

2.1.6. DELIVERABLE. Anything that can be physically delivered, but may include non-manufactured things such as meeting minutes or reports.

2.1.7. KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.8. PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.9. QUALITY ASSURANCE. The Government procedures to verify that services being performed by the contractor are performed according to acceptable standards.

2.1.10. QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.11. QUALITY ASSURANCE SPECIALIST. An official Government representative concerned with matters pertaining to the contract administration process and quality assurance/quality control. Acts as technical advisor to the Contracting Officer in these areas.

2.1.12. QUALITY CONTROL. All necessary measures taken by the contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.13. SUBCONTRACTOR. One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.14. WORK DAY. The number of hours per day the contractor provides services in accordance with the contract.

2.1.15. WORK WEEK. Monday through Friday, unless specified otherwise.

2.1.16 GOVERNMENT-FURNISHED PROPERTY (GFP) OR GOVERNMENT PROPERTY (GP). Property in the possession of, or directly acquired by, the Government and subsequently made available to the contractor.

2.2. ACRONYMS:

ACOMS	Army Commands
ACOR	Alternate Contracting Officer's Representative
AFARS	Army Federal Acquisition Regulation Supplement
AFC	Army Futures Command
ALMS	Army Learning Management System
AMC	Army Material Command
AoA	Analysis of Alternatives
APMS	Army Portfolio Management Solution
AR	Army Regulation
AT	Anti-Terrorism
BLCSE	Battle Lab Collaborative Simulation Environment
CAC	Common Access Card
CBA	Capabilities Based Assessment
CCE	Contracting Center of Excellence
CCP	Concepts and Concept Capability Plans

CCoE	Cyber Center of Excellence
CD	Capability Drop
CDD	Capability Development Document
CDID	Capability Development Integration Directorate
CDRL	Contract Data Requirements List
CEMA	Cyber Electromagnetic Activities
CFR	Code of Federal Regulations
CFT	Cross Functional Team
CG	Commanding General
CO	Cyberspace Operations
CoE	Center of Excellence
COMSEC	Communications Security CONOPS Concept of Operations
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
CRC	CONUS Replacement Component
Cyber SU	Cyberspace Situational Understanding
DA	Department of the Army
DACAP	Department of the Army Cryptographic Access Program
DCO	Defensive Cyberspace Operations
DCR	DOTMLPF Change Request
DD250	Department of Defense Form 250 (Receiving Report)
DD254	Department of Defense Contract Security Requirement List
DFARS	Defense Federal Acquisition Regulation Supplement
DICR	DOTMLPF Integrated Change Request
DMDC	Defense Manpower Data Center
DOD	Department of Defense
DoDD	Department of Defense Directive
DODIN	Department of Defense Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy
EA	Electronic Attack
EAR	Export Administration Regulations
EMSO	Electromagnetic Spectrum Operations
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
FAA	Functional Area Analysis
FAR	Federal Acquisition Regulation
FCC	Futures & Concepts Center
FNA	Functional Needs Analysis
FORSCOM	Forces Command
FSA	Functional Solutions Analysis
FSO	Facility Security Officer
GFP	Government Furnished Property
HIPAA	Health Insurance Portability and Accountability Act of 1996

HQDA	Headquarters Department of the Army
IA	Information Assurance
IAM	Information Assurance Manager
IAVA	Information Assurance Vulnerability Alert
ICD	Initial Capabilities Document
ICDT	Integrated Capability Development Team
ID	Identification
IO	Information Operations
IPT	Integrated Project Team
IRC	Information Related Capabilities
IS	Information System
IS-CDD	Information Systems Capability Development Document
IS-ICD	Information Systems Initial Capabilities Document
IT	Information Technology
ITAR	International Trade in Army Regulations
IW	Information Warfare
JCIDS	Joint Capabilities Integration and Development Systems
JWICS	Joint Worldwide Intelligence Communications System
KO	Contracting Officer
M&S	Modeling and Simulation
MACOM	Major Commands
MTA	Middle-Tier Acquisitions
NETOPS	Network Operations
NISPOM	National Industry Security Program Operating Manual
NRP	Non-Unit Related Personnel
OCI	Organizational Conflict of Interest
OCO	Offensive Cyberspace Operations
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
OPSEC	Operation Security
ORSA	Operations Research and Systems Analysis
OSCOR	On-Site Contracting Officer's Representative
PIPO	Phase In/Phase Out
PNT	Positioning, Navigation, and Timing
POC	Point of Contact
PPBES	Planning, Programming, Budgeting and Execution System
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
QCP	Quality Control Program
RDP	Requirements Development Packet

RFP	Request for Proposal
RHN-E	Regional Hub Node Experimentation
S&T	Science and Technology
SIGACT	Significant Activity
SIPRNET	Secure Internet Protocol Router Network
SPOT	Synchronized Pre-deployment and Operational Tracker
TAA	Total Army Analysis
TE	Technical Exhibit
TO	task order
TR	Tactical Radios
TRADOC	Training and Doctrine Command
TRANSEC	Transmission Security
TTP	Tactics, Techniques, and Procedures

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES:

3.1. Government-Furnished Resources. Government-furnished property, equipment, and services shall be determined at the task order level. If provided, Government-furnished property, equipment, and services shall be used in performance of this contract and its task orders. The Contractor shall account for all property provided by the Government and shall be responsible for the security and condition of said property. Serialized items shall be annotated at the time of issue, with a signature of acknowledgement by the individual Contractor(s). All GFP is the property of the U.S. Government and shall not be transferred to any individual, agency, or public or private entity without the express written approval of the Task Order Contracting Officer. Contractor shall be responsible for, any loss or destruction of, or damage to, items of Government property that are removed from the installation/premises by the Contractor. The contractor shall report loss of government property in accordance with DFARS 252.245-7002. The contractor shall maintain a property management system in accordance with DFARS 252.245-7003. All Government-furnished property will be provided in accordance with FAR 52.245-1 and FAR 52.245-9.

3.2 Facilities: The Government may provide the necessary workspace for the Contractor staff to perform the requirement, to include desk space, telephones, computers, and other items necessary to maintain an office environment. These Government-furnished facilities shall be determined at the task order level. Government-furnished facilities may include: office/work space, office supplies, telephone service, computer access, and storage space. The Government will provide network services (Non-secure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), Defense Switched Network (DSN), Joint Worldwide Intelligence Communications System (JWICS) and other data collection/production/reproduction equipment/software for tasks to be accomplished at Fort Gordon or as specified. The contractor shall maintain the Government facilities in a clean and neat condition. The contractor shall not mark or affix any decals, emblems, or signs portraying the contractor's name or logo to Government facilities. The contractor shall not alter Government facilities without the prior approval of the COR. The contractor shall secure Government facilities when not occupied by contractor personnel.

3.3 Utilities: Utilities may be provided for the Contractor's use in performance of this contract. Government-furnished utilities shall be determined at the task order level. If utilities are furnished, the Contractor shall instruct employees in utilities conservation practices.

3.4 Equipment: The Government equipment will be specified in the individual TOs with specified delivery dates and in specified condition. Office automation

and office supplies may be provided as Government Furnished Equipment (GFE) at the TO level at the discretion of the Government. Non-expendable equipment shall be returned to the Government upon the conclusion of the TO.

3.5 Information: Government-Furnished Information (GFI) relevant to the tasks to be performed under this contract may be provided to the Contractor for use during the performance of the task as specified in the TO (at the discretion of the Government) with specified delivery dates. These documents shall be returned to the Government upon conclusion of the TO.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: The contractor shall furnish all supplies, materials, equipment, facilities, services, and utilities required to perform work under this contract that are not listed under Section 3 of this PWS or specified in task orders issued under the contract.

4.2 Top Secret Facility Clearance: The contractor shall possess and maintain a TOP SECRET facility clearance from the Defense Security Service in accordance with the DD Form 254. The contractor's employees, performing work in support of this contract shall have been granted a security clearance as identified in individual task orders issued under the IDIQ contract from the Defense Industrial Security Clearance Office. The DD 254 is provided as Attachment 2, DD 254 to the solicitation, subsequent DD 254s will be provided for individual task orders issued under the IDIQ contract.

4.3 Training / Certification: The contractor shall provide proof of required training and/or certifications as required by each individual task order under this contract. The contractor shall maintain mandatory training proficiency for period of performance.

4.3.1 Information Assurance (IA) / Information Technology (IT) Certification: Per DoD 8570.01-M (dated 10 Nov 2015), DFARS 252.239.7001 (dated 10 Jan 2008), and AR 25-2 (dated 4 Apr 2019), the contractor employees' supporting IA / IT functions shall be appropriately certified upon task order award. The baseline certification as stipulated in DoD 8570.01-M (dated 10 Nov 2015) shall be completed upon contract award. If proof of training and/or certifications are unavailable on task order start date, COR may accept training plan.

4.4 Contract Management: The contractor shall provide all management, administration, security, quality control, and all else required to ensure successful completion of all deliverables.

PART 5
SPECIFIC TASKS

5. SPECIFIC TASKS: The contractor shall provide general, operational, administrative, and technical support services necessary to accomplish Cyber CDID total capability development tasks. The contractor shall support research, analysis, engineering, drafting, development, coordination, editing, reviewing, staffing, and maintaining any/all deliverable products and capabilities within scope of Force Modernization Proponent (FMP)/Force Proponent areas assigned to the Cyber Center of Excellence.

5.1 Task Area 1: In support of Operations, Administration, and Program Management the contractor shall:

5.1.1 For each task order including Task Area 1 the contractor shall provide a POC as the site lead or program manager. This person (a) shall be present during duty hours, (b) be responsible for overall management of the task, (c) act as the central POC with the COR, and (d) have the authority to act upon or make decisions on all matters pertaining to this contract on behalf of the contractor.

5.1.2 Hold scheduled monthly or ad-hoc meetings/telephone conferences with the COR and/or required Government personnel to review program status. Discussion topics may include, but are not limited to quality control/assurance, deliverables, project schedules, technical progress, any technical difficulties, and travel conducted/planned, and travel resources available.

5.1.3 Provide significant activity reports and program status reports as identified in Part 7 of this PWS.

5.1.4 Plan and conduct In-Progress Reviews (IPR) monthly or as required by the Contracting Officer or Contracting Officer's Representative.

5.1.5 Provide to the Government, non-personal support services in the planning, conducting, and recording of minutes of operational planning teams (OPT), working groups, design assessments, demonstrations, evaluations, assessments, tests, coordination meetings, and synchronization conferences with outside organizations. The contractor shall prepare briefings and presentations for these meetings and executive summaries (EXSUM) upon completion. EXSUMS and/or minutes will be provided to Government within 5 working days of event.

5.1.6 Provide project management subject matter expertise to facilitate Government-led projects and programs. This support shall include contractor personnel capable of providing assistance in:

a. Identifying requirements

b. Addressing the various needs, concerns, and expectations of the stakeholders in planning and executing the project

c. Setting up, maintaining, and carrying out communications among stakeholders that are active, effective, and collaborative in nature

d. Managing stakeholders towards meeting project requirements and creating project deliverables

e. Making recommendations to the Government on the effects of balancing the competing project constraints such as scope, quality, schedule, budget and resources, and risks.

5.1.7 Provide Knowledge Management support to operations of the Cyber CDID HQ and subordinate organizations. This support will include process improvements and management/administration of technical collaboration tools (e.g. SharePoint, MilSuite, InteLink or Microsoft TEAMS…). The contractor shall integrate with internal and external knowledge management teams to integrate information across the organization and enable Cyber CDID to maintain situational awareness of programs and efforts that may impact internal efforts.

5.1.8 Provide support to monitor all ongoing Cyber CDID document and program efforts. This support shall provide the Government with a clear and real-time understanding of the status of documents and programs throughout the organization (e.g. Where a document is in staffing, what are upcoming milestones for document approval, appropriate POC / section responsible for document / program accomplishment, etc.).

5.1.9 Provide non-personal support services support to operations assistance support for Cyber CDID subordinate organizations including management of event calendars, telephonic/electronic/written correspondence management, travel coordination, records management, and general office administration.

5.1.10 Provide on-site Information Technology and Information Security support to the Cyber CDID to include troubleshooting communications and automation systems, installing/repairing computer software and hardware, submitting and responding to trouble tickets, and planning and reporting work schedules.

5.1.11 Cyber Security / Information Assurance (IA) support contractor shall provide information assurance services for all planned, operated and maintained Cyber CDID networks in accordance with procedures outlined in: DoDD 5200.40 – “DoD Information Technology Security Certification and Accreditation Process” (dated 30 Dec 1997); DoD 8570.01-M – “Information Assurance Workforce Improvement Program” (dated 10 Nov 2015); DoD 8140 (dated 12 Jul 2017, the anticipated replacement for DoD 8570 (dated 23 Apr 2015); Department of the

Army Pamphlet 25–2–14 (8 Apr 2019); DoDI 8510.01 (dated 28 Jul 2017); and in AR 25-2 – “Army Cybersecurity” (4 Apr 2019)

5.1.12 Cyber Security / IA Documentation Information Assurance Workforce (IAWF) documentation: certifications; certificates of training; vendor verification system documents; due upon task order award and any change in certification status of IAWF personnel (e.g. new certification, renewal of certification, loss of certification. For newly hired IAWF personnel, IAWF documentation is due prior their first day of work.

5.1.12.1 Coordination & Planning. The contractor shall at a minimum:

a. Publish and Draft updates to the IA/IS Master Plans for Government approval to ensure internal and external security standards are documented and enforced.

b. Provide information to the IAM on the selection, analysis, and effective use of specific security mechanisms.

c. Provide subject matter expertise participation in configuration control boards for the respective systems.

d. Participate in Cyber Security, IA, and IT support coordination meetings as needed and prescribed by the Government IAM.

e. Assist and support Cyber Security / IA initiatives defined by the Government IAM as needed.

5.1.12.2 Systems Compliance. The contractor shall at a minimum and for all specified Cyber CDID information systems:

a. Assist in the Implementation of procedures for vulnerability mitigation, thereby minimizing system threats such as hackers, malicious code attacks, etc. Conduct weekly Information Assurance Vulnerability Alert (IAVA) reviews to determine applicability to specified Cyber CDID hosts, devices, operating systems, and applications, including: automated scans and manual checks for IAVA compliance, analyze the results of the scans and manual checks for compliancy status, and document the findings in a weekly IAVA Compliance Report; mitigation/remediation strategy for each instance of IAVA non-compliance with specified Cyber CDID hosts, devices, operating systems, and applications in a weekly IAVA Compliance Report.

b. Verify operating procedures and accreditation for subject device and/or network;

c. Execute device, network, & system vulnerability assessments using procedures and tools as approved by the Government IAM.

d. Evaluate threats and vulnerabilities to ascertain whether additional safeguards are needed.

e. Develop, analyze, assess for impact, test, and recommend changes to address, mitigate, or eliminate vulnerabilities; execute CCB approved changes.

f. Execute device and/or network security testing to ensure compliance with DoD and U.S. Army standards. Conduct monthly security reviews using available Defense Information Systems Agency (DISA) STIGs to determine applicability and compliance to the specified Cyber CDID hosts, devices, operating systems, and applications, and document the review's results in a monthly STIG Compliance Report. Conduct monthly vulnerability assessments by utilizing the Security Automation Protocol (SCAP) Compliance Checker. Manual checks shall be performed for systems that cannot be checked with an automated tool.

g. Update system documentation to reflect changes and the new status / configuration of the system.

h. Ensure the development of system certification documentation by reviewing and endorsing such documentation and recommending action by the Government IAM and the Director.

i. Maintain appropriate system accreditation documentation, including records in standard Army IT/IA tracking tools (e.g. Army Portfolio Management Solution (APMS), Certification and Accrditaiton (C&A) Technoloy Database (TdB), etc.). Evaluate certification documentation and provide written recommendations for accreditation to the IAM.

j. Ensure records of all security-related vulnerabilities and incidents are maintained and report serious or unresolved violations to the IAM.

k. Assess changes in the systems, networks, its environment and operational needs that could impact the security posture and/or accreditation of the systems.

l. Document and research incident resolutions and communication with all appropriate parties as directed by the Government IAM.

m. Provide Intrusion Detection System/Intrusion Prevention System installation and policy Review.

n. Research security related regulations, publications and directions to stay abreast so potential threats to the specified Cyber CDID computers may be effectively mitigated.

o. Recommend, develop, and coordinate staffing of interconnection agreements with external systems.

5.1.12.3 User Compliance. The contractor shall at a minimum and for all specified Cyber CDID information systems:

a. Ensure that all user requests for system access are staffed and processed according to organizational procedures, as prescribed by the Government IAM.

b. Ensure that all system users complete & renew at least annually the Acceptable Use Policy (AUP) required for each system accessed. A single AUP may be applicable to multiple systems. Maintain a repository of all AUPs.

c. Ensure that all user requests for privileged (aka elevated) access to systems are staffed and processed according to organizational procedures, as prescribed by the Government IAM.

d. Ensure that all privileged system users complete & renew at least annually the Privileged-level Access Agreement (PAA) required for each system accessed. A single PAA may be applicable to multiple systems. Maintain a repository of all PAAs.

e. It is DoD policy that all privileged users and IA managers shall be fully qualified per DoD Instruction 8500.02, "Information Assurance (IA) Implementation," (dated 28 Jul 2017), trained, and certified to DoD baseline requirements to perform their IA duties. In order to maintain certifications as current and active, contractor personnel shall complete continuing education requirements in accordance with the regulations listed above and document them at the direction of the Government IAM. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

f. Manage & provide IA training and certification documentation via standard DoD, Army, and vendor tracking tools & databases (e.g. ATCTS; DMDC), as prescribed by the Government IAM.

5.1.12.4 Incident Response. The contractor shall at a minimum and for specified Cyber CDID information systems:

a. Immediately notify the Government IAM & branch chief of any: information security incident; discovery of a condition that impacts the security posture or accreditation status of the system. Examples include but are not limited to:

1. Known or suspected intrusion or access by an unauthorized individual.
2. Authorized user attempting to circumvent security procedures or elevate access privileges.
3. Unexplained modifications of files, software, or programs.
4. Unexplained or erratic IS system responses.
5. Presence of suspicious files, shortcuts, or programs.
6 Malicious logic infection (ex., virus, worm, trojan).
7. Receipt of suspicious e-mail attachments, files, or links.

b. At the direction of the Government IAM & branch chief, coordinate response actions and notification to appropriate parties.

5.1.13 Digital Graphic Design. The contractor shall provide support for concept, Concept of Operations (CONOPS), and requirement document development by designing graphical presentations and utilizing products including Microsoft (MS) Office (especially PowerPoint) and Adobe Creative Suite that depict integrated signal, cyber, information warfare (IW) and electronic warfare (EW) concepts to visitors, senior leadership, and stakeholders. The contractor shall develop and create images such as organizational diagrams and visualizations of integrated signals, EW, IW, and cyberspace operating concepts that enable better understanding of complex ideas. The contractor shall create concepts from start to finish in a collaborative environment with attention to detail. The contractor shall display creativity and clarity in designs, layout, and display. Majority of tasks will be focused on print products to include text formatting, charts, matrices, graphs, photos, and map compilation. The contractor shall be able to learn quickly, think creatively, solve problems, and possess good writing skills.

5.2 Task Area 2: In support of Experimentation and Capability Evaluation, the contractor shall:

5.2.1 For each task order including Task Area 2, the contractor shall provide a POC as the site lead or program manager. This person (a) shall be present during duty hours, (b) be responsible for overall management of the task, (c) act as the central POC with the COR, and (d) have the authority to act upon or make decisions on all matters pertaining to this contract on behalf of the contractor.

5.2.2 Provide support to Cyber CDID for capability evaluations, assessment, exercises, risk reduction, and test events. These evaluations may include live, constructive, virtual, table-top, and other experiments and demonstrations that may inform capability development.

5.2.3 Support efforts to ensure all assigned capabilities are meeting all operational requirements; coordinate with Materiel Developers, Test, and Evaluation organizations to provide subject matter expertise for evaluations and operational tests, review and provide feedback on test and evaluations documents such as Test and Evaluation Master Plans, System Evaluation Plans, Operational Test Plans, and serve as a participant in Reliability, Availability, and Maintainability Assessment Conferences.

5.2.4 Develop, gain approval for, coordinate, ensure preparation, and monitor all DOTMLPF-P equites, test requirements, standards, scenarios, threat assessments, and activates related to system testing and evaluation.

5.2.5 Develop and review critical drivers for experimentation / assessments to include operational mission threads, applicable scenarios, and learning demands.

5.2.6 Collaborate with materiel developers and the test community in the development of System Engineering Plans and Test and Evaluation Management Plans by assisting the PM with the identification and assessment of essential elements of analysis; and act as a member of a team consisting of functional, training, operations, and T&E experts to execute the test event.

5.2.7 In support of CEMA Experimentation Execution the contractor shall:

5.2.7.1 The contractor shall identify US Army requirements, Tactics, Techniques, and Procedures (TTPs), CONOPS for implementation and use of Signal, Cyber, and EW technologies on the battlefield. Using TRADOC Pamphlet 71-20 (dated 3 May 2013) and Government provided templates, the contractor shall write detailed Experimentation Plans. Contractor work shall include the development of: experimentation data collection plans; research; equipment configuration; prototyping of solutions to support operational capability gaps. In particular, the contractor shall investigate emerging technologies that support Signal, Cyberspace, EW, and Information Related missions in austere environments utilizing emerging technologies.

5.2.7.2 Signals and Network Analysis. The contractor shall play a key role in developing the Signals based experimentation and analysis capability within the Cyber CDID. The contractor must be able to think strategically to develop future capabilities as well as provide solutions to current problems, based upon operational Signals experience. The contractor must anticipate working on commercial networks, as well as military, tactical, and enterprise networks. The contractor will work closely with Army Capability Manager Tactical Radio (ACM-TR) and Army Capability Manager Networks and Services (ACM-NS) to inform, develop, and validate requirements within the JCIDS. The analysis conducted will be used to inform, develop, and validate requirements through experimentation

independently or in coordination with ACM-TR and/or ACM-NS. The Signal Analyst will explore current Army Signals posture, determine needs, assess risks, vulnerabilities, and recommend countermeasures. Signal analysts will employ a thorough understanding of the tenets of Signal operations and know how to optimally` use all Signal resources. Signals analysts will develop capabilities that will deliver tactical, operational, and strategic advantages. The contractors shall plan, lead, and/or coordinate meetings as needed to ensure completion of all project objectives.

5.2.7.3 Cyber Warfare (CW) Analysis. The contractor shall play a key role in supporting the CW experimentation and analysis capability within the Cyber CDID. The contractor must be able to think strategically to develop future capabilities as well as provide solutions to current problems, based upon operational Cyber Warfare Experience. The contractors must anticipate working in Commercial Networks as well as Military Tactical and Enterprise networks. Cyber Warfare Analysts will work closely with Army Capability Manager Cyber (ACM-Cyber) to inform, develop, and validate requirements within the JCIDS. The analysis conducted will be required to inform, develop, and validate requirements through experimentation independently or in coordination with ACM-Cyber. The Cyber Warfare Analyst will explore current Army CW posture, determine needs, assess risks, vulnerabilities, and recommend countermeasures. CW analysts will employ a thorough understanding of the tenets of Cyber Network Operations (CNO), and know how to optimally use all CNO resources for “effects-based” cyber warfare. CW analysts will develop CNO capabilities that will deliver tactical, operational, and strategic advantages. The CW contractors shall plan, lead, and/or coordinate meetings as needed to ensure completion of all project objectives.

5.2.7.4 EW Analysis. The contractor shall play a key role in supporting the EW experimentation and analysis capability within the Cyber CDID. The contractor must be able to think strategically to develop future capabilities, while also providing solutions to current problems utilizing operational EW experience. The contractor is expected to work with Commercial, Military, Tactical, and Enterprise networks. EW contractors shall work closely with Army Capability Manager EW (ACM-EW) to inform, develop, and validate requirements within the JCIDS. EW contractors shall inform and validate requirements through experimentation. EW contractors shall evaluate JCIDS requirement documents independently or in coordination with ACM-EW. EW contractors shall analyze current Army EW requirements and determine future experimentation needs. EW contractors shall assess EW risks and vulnerabilities and recommend countermeasures. The EW contractors shall plan, lead, and/or coordinate meetings as needed to ensure completion of all project objectives.

5.2.7.5 Information Related Capability Analysis. The contractor shall play a key role in supporting the Information Related experimentation and analysis capability within the Cyber CDID. The contractor must be able to think

strategically to develop future capabilities, while also providing solutions to current problems utilizing operational Information experience. The contractor is expected to work with Commercial, Military, Tactical, and Enterprise networks. Contractors shall work closely with the Cyber-CDID, Signal School, and Cyber School to inform, develop, and validate requirements within the JCIDS. Contractors shall inform and validate requirements through experimentation. Contractors shall evaluate JCIDS requirement documents independently or in coordination with assigned document sponsor. Contractors shall analyze current Army Information requirements and determine future experimentation needs. Contractors shall assess risks and vulnerabilities and recommend countermeasures to operations and capabilities within the information environment. The contractors shall plan, lead, and/or coordinate meetings as needed to ensure completion of all project objectives.

5.3 Task Area 3: In support of Concept Development, the contractor shall:

5.3.1 For each task order including Task Area 3, the contractor shall provide a POC as the site lead or program manager. This person (a) shall be present during duty hours, (b) be responsible for overall management of the task, (c) act as the central POC with the COR, and (d) have the authority to act upon or make decisions on all matters pertaining to this contract on behalf of the contractor.

5.3.2 Provide Subject Matter Expertise, Information Operations, Signal, and Cyber/Electronic Warfare for concept development efforts. The contractor will develop strategic future capabilities, while also providing solutions to current problems utilizing operational experience.

5.3.3 The contractor shall work with Commercial, Military, Tactical, and Enterprise networks. Contractors shall work closely with the Cyber-CDID, Signal School, and Cyber School to inform, develop Army and Joint Concept documents.

5.3.4 Develop written products such as studies, white papers, Joint and Army supporting and functional concepts. The contractor will be part of a writing team that varies by concept of development effort. The Future and Concepts Center's Annual Modernization Guidance (AMG) directs certain activities to support concept development; the contractor as part of the writing team lead may request other activities as needed.

5.3.5 Review emerging Army Capstone and Operating Concepts for impacts on Functional Concepts and Concepts and Concept Capability Plans (CCP) and provide written report and/or briefing.

5.4 Task Area 4: In support of Requirement Development, the contractor shall:

5.4.1 For each task order including Task Area 4, the contractor shall provide a POC as the site lead or program manager. This person (a) shall be present during duty hours, (b) be responsible for overall management of the task, (c) act as the central POC with the COR, and (d) have the authority to act upon or make decisions on all matters pertaining to this contract on behalf of the contractor.

5.4.2 Support planning for Signal, Cyberspace Operations, Electronic Warfare, and/or Information Related capabilities, programs, projects, and systems including determining operational requirements and technologies needed to satisfy them. Develop Life-Cycle system documentation to translate approved requirements into funded programs/projects. Develop, write, review, integrate, and staff JCIDS documents. DOTMLPF-P solutions for assigned capabilities.

5.4.3 Assist in developing, writing, assessing, integrating, staffing, and documenting Cyber CDID visions, strategies, concepts, and Capabilities Based Analysis (CBA) into appropriate JCIDS products (including supporting documentation) to include, but not limited to Initial Capabilities Documents (ICD), Capabilities Development Documents (CDD), Requirements Definition Packages (RDP), Capability Drops (CD), and DOTMLPF Integrated Capabilities Recommendation (DICR).

5.4.4 Support Integrated Capabilities Development Teams (ICDT), Cross Functional Teams, working groups, and stakeholder communities as necessary for successful coordination, staffing, and validation of JCIDS products and documents.

5.4.5 Support the Cyber CDID by providing research, technical analysis, and technical writing support to architectural documents and products. The work includes:

a. Developing OA products, as described in the most recent DOD architecture framework (DODAF)

b. Coordinating and attending working groups and providing support to Concept Development and analysis via the architecture process

c. Researching and providing architecture related products for use in capability development and JCIDS documents

5.4.6 Research and monitor emerging technologies from Government, industry, academia, and other sources for the purposes of gap/opportunity identification, requirements development, and capability modernization.

5.5 Task Area 5: In support of Analysis, the contractor shall:

5.5.1 For each task order including Task Area 5, the contractor shall provide a POC as the site lead or program manager. This person (a) shall be present during duty hours, (b) be responsible for overall management of the task, (c) act as the central POC with the COR, and (d) have the authority to act upon or make decisions on all matters pertaining to this contract on behalf of the contractor.

5.5.2 Provide on-site dedicated operations research and systems analysis (ORSA) support including technical and analytical expertise in Signal/Communication Networks & Information Services (e.g. combat-net radio, software defined radio systems, network transport, information systems and services, telecommunications, communications security, transmissions security, network operations), Cyberspace Operations (e.g. Offensive Cyberspace Operations, Defensive Cyberspace Operations, and Cyberspace Situational Understanding), Electronic Warfare (e.g. Electronic Attack, Electronic Protection, and Operations in the Information Environment

5.5.3 The contractor shall utilize the Study Planning process to perform studies and analyses to refine operational concepts and system-specific requirements. Within the study planning process, the contractor will identify the best analytical method(s) to support the problem being studied.

5.5.4 Develop written products such as analysis insights for individual exercises or final reports for larger, more prolonged analytical events.

5.5.5 The contractor shall review and provide written comments to ensure the organizational design of Modular Forces is consistent with the design parameters in the Operational & Organizational (O&O) concepts.

5.6 Task Area 6: In support of FMP Integration, the contractor shall:

5.6.1 For each task order including Task Area 6, the contractor shall provide a POC as the site lead or program manager. This person (a) shall be present during duty hours, (b) be responsible for overall management of the task, (c) act as the central POC with the COR, and (d) have the authority to act upon or make decisions on all matters pertaining to this contract on behalf of the contractor.

5.6.2 Assess capability gaps and changes in systems/force structure to identify required DOTMLPF changes.

a. Doctrine: Monitor and ensure currency and relevancy of Signal, Cyberspace Operations, Electronic Warfare, or Information Related Capabilities' doctrine and concepts for current and future forces.

b. Organization: Monitor, track, and update Signal, Cyberspace Operations, Electronic Warfare, or Information Related Capabilities'

force design ensuring current, proposed, and future tables of organization and equipment reflect the needs identified by organizational echelons.

c. Training: Monitor development of Signal, Cyberspace Operations, Electronic Warfare, or Information Related Capabilities individual and collective tasks, combined arms training strategies at the CTCs and in schools, and low-density home station training needs.

d. Leader Development: Monitor and ensure relevant Signal, Cyberspace Operations, Electronic Warfare, or Information Related Capabilities professional development at CTCs and in training institutions.

e. Materiel: Serve as Army's primary Signal, Cyberspace Operations, Electronic Warfare, or Information Related Capabilities user representative and stakeholder for materiel system development and integration.

f. Personnel: Monitor updates to and ensure relevancy of military occupational specialties, additional skill identifiers, functional areas, career paths, and specialties through collaboration with force modernization and branch proponents.

g. Facilities: Ensure common understanding across the Army's decision making authorities of the need for and the availability of required training facilities and ranges for assigned capabilities, for both the operational and institutional Army.

e. Policy: Identify policy issues that require change, and submit recommended changes to Department of Defense or international policy that may be changed to close or mitigate capability gaps.

5.6.3 Provide subject matter expertise for operational and other testing events as needed to the Data Authentication Group to authenticate and validate data collected during test and evaluation events.

5.6.4 Provide input to the Government in the development of Integrated Logistics Support (ILS) and Reliability, and Maintainability (RAM) portions of test plans; evaluation of Integrated Logistics Support and RAM characteristics of systems

5.6.5 Develop and validate operational mission threads for baseline systems, technologies, and Force Modernization Proponent areas supported by the Cyber CDID. Specifically, the contractor shall support the Cyber CDID to integrate baseline system capabilities into system-of-systems interoperability testing and application testing. The development and validation of operational mission

threads shall also ensure that collective training for certification and unit fielding are consistent with program requirements or other capacities.

5.6.6 Provide the necessary analytical and/or engineering labor to perform capability management and integration of DoD and Army acquisition programs for Signal, Cyberspace Operations, Electronic Warfare and Information Related capabilities. Field support to include observation, data collection, analysis to inform modernization and DOTMLPF-P integration.

5.6.7 Analyze assigned capabilities, develop operational architectures, and update unit's/formations basis of issue in full coordination with all Centers of Excellence, as well as Operational Units, FORSCOM and HQDA to determine recommended fielding quantities and placement in formations.

5.6.8 Provide support to fielded units. This shall include resolving issues from the field, assisting with re-fresher training, updating and providing TTP training, and assisting units as they employ Signal, Cyberspace Operations, Electronic Warfare, or Information Related Capabilities.

5.6.9 Provide the necessary analytical and/or engineering labor to perform Capabilities Based Assessments. Research and determine applicable strategy and concepts documents. Identify applicable required capabilities. Decompose required capabilities into tasks linked to the Army Universal Task List or Universal Joint Task List. Assess task standards in designated scenarios against fielded or planned capabilities to determine capability gaps. Identify potential DOTMLPF solutions to close or mitigate identified capability gaps.

5.6.10 Assess, develop, review, and modify basis of issue guidance to describe operational attributes of assigned materiel solutions and support development of the capability's Basis of Issue Plan (BOIP).

5.7. SERVICE CONTRACT REPORTING : The contractor shall report the total dollar amount invoiced for services performed during the previous Government fiscal year under the order, the number of Contractor direct labor hours expended on the services performed during the previous Government fiscal year, and data reported by subcontractors when applicable. This information shall be submitted via the internet at www.sam.gov.

Reporting inputs shall be for the labor executed during the period of performance during each Government FY, which runs from 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.

5.8. Invoicing:

5.8.1 Format. All invoices shall be submitted in Procurement Integrated Enterprise /Environment (PIEE) Wide Area Workflow (WAWF) as a 2-in-1 invoice with all applicable monthly documentation attached. Monthly documentation includes Monthly Status Reports (MSR), In- Progress Reviews (IPR), Trip Reports, and other reports where applicable as stated in the PWS. Monthly documentation may not be submitted via email. Invoices submitted as anything other than a 2-in-1 and / or without attached monthly documentation will be rejected.

5.9.2 Payment for Travel. If the contractor is requesting payment for travel during the month of the submitted invoice, the Trip Report, along with supporting documentation shall accompany that invoice in order to receive payment for travel. Supporting documentation includes lodging, gas, airline, rental car, parking receipts, etc. If the electronic file containing supporting documentation is too large to be attached, please arrange with the COR to submit those documents via email.

5.9.3 Authority: A contractor with the authority to bind the company contractually shall certify all invoices. Invoices shall be submitted no later than five days after the end of each month (30-day period), depending on the task order award date. Failure to submit invoices in a timely manner is a direct violation of this contract agreement. The Government will have the right to exercise a penalty cost, due to the contractor being out of compliance of this contract agreement.

5.9.4 Final Invoice: All invoices submitted at the end of the period of performance (each year) shall state “final invoice” and be clearly marked as base period, option period 1, option period 2. This annotation shall be accomplished in Wide Area Workflow Invoice 2-in-1 section, under Tab Misc. Info, and in the area of Initiator Information Comments.

PART 6
APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS:

6.1 The contractor (to include subcontractors) must abide by all applicable regulations, publications, manuals, and local policies and procedures. The Government, for use in accomplishing specified tasks, will supply supporting documentation required to accomplish specific requirements and products described in this contract and all task orders issued under this contract. The contractor shall perform tasks IAW applicable Government regulations and in compliance with listed Army Regulations (AR), Field Manual (FM) and technical publications. Applicable documentation may include, but not limited to the following:

- AR 25-1, dated 15 July 2019, Army Information Technology
- AR 25-2, dated 4 Apr 2019, Army Cybersecurity
- AR 25-50, dated 17 May 2013, Preparing and Managing Correspondence
- AR 71-9, dated 15 Aug 2019, Warfighting Capabilities Determination
- AR 190-11, dated 17 Jan 2019, Physical Security of Arms, Ammunition, and Explosives
- AR 190-13, dated 27 Jun 2019, The Army Physical Security Program
- AR 190-51, dated 27 Jun 2019, Security of Unclassified Army Resources (Sensitive and Non-sensitive)
- AR 350-1, dates 12 Aug 2019, Army Training and Leader Development; http://armypubs.army.mil/epubs/350_Series_Collection_1.html
- AR 380-5, dated 22 Oct 2019, Department of the Army Information Security Program
- AR 380-53, dated 17 Jan 2013 – Communications Security Monitoring
- AR 525-13, dated 3 Dec 2019, Antiterrorism
- AR 530-1, dated 26 Sep 2014, Operations Security
- AR 710-2, dated 28 Mar 2008, Supply Policy Below the National Level
- AR 715-9, 20 Jun 2011, Operational Contract Support Planning and Management
- AR 735-5, dated 9 Nov 2016, Property Accountability Policies
- ATP 6-01.1, dated 06 Mar 2015, Techniques for Effective Knowledge Management
- Chairman Joint Chief of Staff Manual (CJCSM) 3500.04E, Universal Joint Task List (UJTL), dated 25 Aug 2008
- CJCSI 6510.01F, dated 09 Jun 2015- Information Assurance (IA) And Computer Network Defense (CND)
- CJCSI 5123.01H, dated 31 Aug 2018, Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the JCIDS,
- CJCSM 6510.01B, dated 18 Dec 2014 - Cyber (Incident Handling Program)

- CNSSI 1253, 27 March 2014, Security Categorization and Control Selection for National Security Systems
- DA PAM 25-2-14, dated 08 Apr 2019, Risk Management Framework
- DFARS 252.239-7001, 10 Jan 2008, Information Assurance Contractor Training and Certification
- DoD 5200.01, Vol 1,2,3,4, dated 24 Feb 2012, DOD Information Security Program
- DoD 5200.2-R, dated 23 Feb 1996, Personnel Security Program
- DoD 8500.01, dated 14 March 2014, Cybersecurity
- DoD 8530.1-M, dated 25 Jul 2017 – Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process Program Manual.
- DoD 8530-1, dated 10 Oct 2019 - Computer Network Defense (CND) Directive
- DoD 8570.01-M, dated 10 Nov 2015- Information Assurance Workforce Improvement Program
- DoD Cybersecurity Policy Chart: http://iac.dtic.mil/csiac/ia_policychart.html, dated 30 Jul 2020
- DoD Directive 5105.21, Vol 1,2,3, dated 19 Oct 2012 - Department of Defense Manual Sensitive Compartmented Information (SCI) Administrative Security Manual
- DoDD 5200.40, DoD Information Technology Security Certification and Accreditation Process
- DoDD 8140.01, dated 31 Jul 2017, Cyberspace Workforce Management
- DoD Directive 8570, dated 23 Apr 2015 DoD Approved 8570 Baseline Certifications
- DoD Instruction 8510.01, dated 28 Jul 2017; Risk Management Framework (RMF) for DoD Information Technology (IT)
- DoD Manual 5220.22-M, Ch1, 18 May 2016, National Industrial Security Program Operating Manual (NISPOM)
- DoDI 8500.2, dated 1 Jul 2012 - Information Assurance (IA) Implementation
- Department Defense (DoD) Unified Capabilities (UC) Reference Architecture v1, dated 11 Oct 2013
- Joint Publication 3-1, dated 8 Jun 2018, Cyberspace Operations
- Federal Acquisition Regulation (FAR) 31.205-46, dated 08 Aug 2020, Travel Costs
- Field Manual 3-0, dated 6 Dec 2017, Operations
- FM 3-38, dated 12 Feb 2014, Cyber Electromagnetic Activities (CEMA)
- FM 6-0, dated 22 Apr 2016, Commander and Staff Organization and Operations
- FM 6-02, dated 13 Sep 2019, Signal Support to Operations
- FM 7-15, dated 9 Dec 2011, The Army Universal Task List
- FM 7.0, dated 23 Aug 2012, Training the Full Spectrum OPS;
- ICD 503, 21 July 2015, IC Information Technology Systems Security Risk Management

- ICD 705, dated 1 Oct 2013, Sensitive Compartmented Information Facilities
- IT Box “The Information Technology (IT) Box A Primer,” dated 19 Aug 2016
- JP 3.0 Joint Operations, dated 1 Jan 2019
- JP 3-12 Cyberspace Operations, dated 8 Jun 2018
- JP 6-0 Joint Communications System, dated 4 Oct 2019
- JP 6-01 Joint Electromagnetic Spectrum Management Operations, dated 20 Mar 2012
- Joint Travel Regulations (JTR), dated 1 Aug 2020
- Manual for the Operation of the Joint Capabilities and Development System (JCIDS), dated 31 Aug 2018. Link: https://www.acq.osd.mil/jrac/docs/2018-JCIDS.pdf
- NIST SP 800-37 r1, dated 5 Jun 2014 Guide for Applying the Risk Management Framework to Federal Information Systems
- NIST SP 800-53 r4, dated 22 Jan 2015, Security and Privacy Controls for Federal Information Systems and Organizations
- TRADOC Pamphlet 350-70-12, dated 03 May 2013 – The Army Distributed Learning (DL) Guide
- TRADOC Regulation 71-20, dated 28 Jun 2013, Concept Development, Capabilities Determination, and Capabilities Integration.
- TRADOC Regulation 350-70, dated 10 Jul 2017, Army Learning Policy and Systems
- TRADOC Pamphlet 525-3-3, U.S. Army Functional Concept for Mission Command 2016-2028, dated 13 Oct 2010
- TRADOC Pamphlet 525-7-8, The United States Army’s Cyberspace Operations Concept Capability Plan 2016-2028, dated 22 Apr 2010
- USASC&FG 350-22, dated 01 Mar 2007, (Test Control Policies and Procedures).
- USASC&FG 350-5, 23 Jan 2014, (Ft Gordon Academic Practices)

PART 7
DELIVERABLES SCHEDULE

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
QCP (paragraph 1.6.1)	Within 30 days of contract performance start	1	Email, MS Office document, or on-line Collaboration tool.	COR
Program Status Report (paragraph 5.1, 7.1)	Monthly or within five (5) working days of request	1	(routine) Submitted in WAWF (upon request) email, MS Office document, or on-line Collaboration tool	COR and / or Gov rep
Personnel Training Requirement Documentation (paragraph 1.6.10.1, 5.2.1.13.1, 7.2)	Once per Task Order Start or within five (5) working days of new hire	1	Email, MS Office document, or on-line Collaboration tool	COR
IPR (paragraph 5.14)	Upon government request or IAW TO PWS.	1	Email, MS Office document, on-line Collaboration tool, or event at the discretion of the Gov project lead	
Document Status Report (paragraph 5.1, 7.3)	Monthly or within one (1) working day of request	1	Email, MS Office document, or on-line Collaboration tool	COR and / or Gov rep
Significant Activity Report (paragraphs 1.6.13.1 and 5.1, 7.4)	Within five (5) working days of significant activity	1	Email, MS Office document, or on-line Collaboration tool	Gov rep
Operations Product (paragraph 5.1, 5.1.13.2 7.5)	Upon government request or IAW TO PWS.	1	Email, MS Office document, on-line Collaboration tool, or event at the discretion of the Gov project lead	Gov rep
Experimentation Product (paragraph 5.2, 7.6)	Upon government request or IAW TO PWS.	1	Email, MS Office document, on-line Collaboration tool, or event at the discretion of the Gov project lead	Gov rep
Concept Product (paragraph 5.3, 7.7)	Upon government request or IAW TO PWS.	1	Email, MS Office document, on-line Collaboration tool, or event at the discretion of the Gov project lead	Gov rep
Requirement Product (paragraph 5.4, 7.8)	Upon government request or IAW TO PWS.	1	Email, MS Office document, or on-line Collaboration tool at the discretion of the Gov project lead	Gov rep
Analytical Report (paragraph 5.5, 7.9)	Upon government request or IAW TO PWS.	1	Email, MS Office document, or on-line Collaboration tool at the discretion of the Gov project lead	Gov rep
Force Proponent Integration Product (paragraph 5.6, 7.10)	Upon government request or IAW TO PWS.	1	Email, MS Office document, or on-line Collaboration tool at the discretion of the Gov project lead	Gov rep

7.1 The Deliverables Schedule is an overview of associated functions that are deliverable/reportable by the contractor for the MATOC. A more detailed, inclusive deliverables list will be issued with each Task Order. The deliverables list will specifically outline each function and the Government's expectations of contractor performance.

7.2 Program Status Report: The contractor shall provide progress reports to the COR on the status of program efforts summarizing cumulative work accomplished, personnel status, difficulties encountered, work planned for the next month, and resourcing. Reports shall be delivered on or before the 5th day following the end of each month and within five working days upon request. The report shall include:

a. A front cover sheet which includes the contractor's name and address, the contract number, the nomenclature of the system or program, the date of the report, the period covered by the report, the title of the report, tasks covered by the report, and the name of the issuing Government activity;

b. Description cumulative deliverable products provided to the Government;

c. Description of activities/deliverables planned for the following reporting period;

d. Monthly Travel Expenses, roll up of the overall travel budget, and planned/forecasted travel budget through PoP end;

e. Problem areas affecting technical or scheduling elements, with background and any recommendations for solutions beyond the scope of the contract;

f. Any significant changes to the contractor's organization or method of operation to the project management network, or to the milestone chart;

g. Results, positive or negative, obtained related to previously-identified problem area, with conclusions and recommendations;

h. Name and telephone number of preparer of the report;

i. Appendixes for any necessary tables, references, photographs, illustrations, and charts.

7.3 Personnel Training Requirement Documentation: The contractor shall provide the Contracting Officer representative proof of education, training, qualifications, and verification of security clearance for all contractor employees prior to contract start date and when new contractor employees are hired. COR will inform contractor if necessary qualifications are not adequately documented. Upon notification of inadequately documented qualifications the contractor shall provide additional documentation within five (5) working days (or longer with approval of COR) or replace contractor employee with qualified substitute.

7.4 Document Status Report: The contractor shall maintain an up-to-date tracking list of all applicable programs and documents in the Cyber CDID. This product shall enable the Government to easily identify what documents and programs are being developed/reviewed/validated by Government and contract personnel and serve as a tool to track documents throughout staffing processes, identify issues, and communicate ongoing efforts internally and externally.

a. Document / program name

b. Document / program type

c. Milestones and key dates

d. Approval requirements

e. Responsible section

f. Other data as determined by the Government

7.5 Significant Activity Report: Contractors shall provide to the Government a Significant Activity Report (SAR). The SAR is a concise description of an action or event (e.g. briefings, workshops, contractor travel, etc.). The report shall contain the following:

a. Title of the event/significant activity

b. Name(s) of personnel involved

b. A brief summary of the objective

c. Relevant background

d. Time period

e. Location

f. If significant activity involved contractor travel provide a summary of individual travelers, projected cost from approved travel authorization, and a summary of actual costs incurred.

e. Conclusion and recommendations suggested at the event

f. Potential impact on past, current, or planned CCoE efforts/products

g. Name, email, and telephone number of preparer of report

7.6 Operations Product: As required, the contractor shall prepare products from Cyber CDID Capability Development activities. Products may include information/white papers, briefings, comment resolution matrices, travel authorizations/vouchers, trouble tickets, editorial comments, document revisions, correspondence, event calendars, and synchronization matrices. Additional information provided in individual task orders.

7.7 Experimentation Product: As required, the contractor shall prepare products for or resulting from research, experimentation, or exercises where science, technology, and/or DOTMLPF capability evaluation is being accomplished. The contractor shall develop reports in coordination Gov project lead requirements and submitted on time in the required format. Additional information provided in individual task orders.

7.8 Concept Product: As required, the contractor shall prepare products relating to the proponent conceptual special studies and analyses, live, constructive and virtual war games. Products may include functional or operational concept documents, capability specific concepts of operations/employment, or scenarios/vignettes. The contractor shall develop reports in coordination Gov project lead requirements and submitted on time in the required format. Additional information provided in individual task orders.

7.9 Requirement Product: As required, the contractor shall provide products identifying the need for a materiel approach, non-materiel approach, or an approach that is a combination of materiel and non-materiel to mitigate or close specific capability gap(s). The contractor shall develop products formats identified in JCIDS unless otherwise directed by Gov rep. Additional information provided in individual task orders.

7.10 Analytical Report: As required, the contractor shall provide research, analytical support, and documentation in formats defined by Gov project lead. These support documents shall be submitted on time and in the required format.

7.11 Force Proponent Integration Product: As required, the contractor shall provide analysis and documentation to assist the Government in accomplishing required maintenance and modernization of program of record equipment. These documents shall be submitted on time and in the required format. Additional information provided in individual task orders.

PART 8
PERFORMANCE REQUIREMENT SUMMARY (PRS)

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective	Performance Standard	Performance Threshold	Method of Surveillance	Incentive/ Disincentive
PRS #1 The contractor shall provide Program Status Report (paragraph 7.1)	Reports delivered on or before the 5th day following the end of each month and within five (5) working days upon request. Reports include all information required in paragraph 7.1 of this PWS.	No more than one report is 2 days late.	100% Inspection	Poor performance will be reflected in CPARS Report; Compliant performance will result in positive CPARS Narrative
PRS # 2 The contractor shall comply with FAR 52.228-5 "Insurance – Work on a Government Installation"	Contractor provides Certificate of Insurance Annually	No more than one report is 2 days late.	100% Inspection	Poor performance will be reflected in CPARS Report; Compliant performance will result in positive CPARS Narrative
PRS #3 The contractor shall comply with all security requirements. (paragraph 1.6.7 including all sub-paragraphs and as specified in TOs)	Contractor adheres to PWS requirements	Provided at proposal submission, and maintained for the life of the contract and issued task orders	100% Inspection	Poor performance will be reflected in CPARS Report; Compliant performance will result in positive CPARS Narrative
PRS #4 The contractor shall provide qualified personnel, equipment, supplies, transportation, materials,	Personnel are qualified, with appropriate skills and experience. Effective management was provided to all personnel, to include the selection, retention, training, support, and replacement, when necessary. Continuity of support is maintained.	Personnel are qualified with appropriate skills and experience. Support is adequately staffed. Performance	100% Inspection	Poor performance will be reflected in monthly and CPARS reports and may negatively impact performance incentives;

supervision, and other items for each TO for each specified task area. (paragraph 5 including all sub-paragraphs)	Contractor delivery of products and/or services meets all contract requirements. Problems that are encountered are minor and resolved in a prompt, satisfactory manner. Contract requirements met with little rework/re-performance required and with few minor and no significant problems encountered. Performance meets all technical and functional requirements, and is highly responsive to changes in technical direction and/or the technical support environment.	occurs with minimal required re-performance/ re-work and services meet all contract requirements.		Compliant performance will result in positive monthly and CPARS reports, and may positively impact performance incentives
PRS #5 The contractor shall provide a Quality Control Plan for this contract and all task orders to this contract (paragraph 1.6.1)	Contractor provides Quality Control Plan	No more than one report is 2 days late.	100% Inspection	Poor performance will be reflected in CPARS Report; Compliant performance will result in positive CPARS Narrative

Measurable performance standards in terms of quality, timeliness, quantity and the method of assessing contractor performance against each performance standard will be addressed in the Performance Requirements Summary (PRS) within each individual Task Order Request.

Appendix A
Specific Qualification Requirements

Specific Qualification Requirements are listed below for reference. These labor categories include the labor mix that the Government currently envisions for use in task orders under these task areas, and any MA IDIQ holder must be able to provide personnel with these qualifications under TOs; however, specific labor mix and specific qualifications/education/experience will be determined for each task order. When requiring experience in preceding years, preceding years refers to the time prior to issuance of the individual Task Order Request.

A-1Program Manager
Experience: At least ten (10) years management experience or equivalent on similar Government contracts
Education: Undergraduate degree from an accredited institution.
Proficiencies: Be proficient in conflict resolution. Be able to communicate orally and in writing with COR. Possess the skill sets to supervise contractor employees. Be capable of coordinating work schedules/assignments of contractor employees. Be knowledgeable of all aspects of assigned contract to include but not limited to deliverables, costs, quality control plan, and security requirements.
Qualifications: Active Project Management Professional (PMP) training at a minimum. Shall provide a resume outlining program management experience, education, and qualifications.
Security: Possess a Top Secret security clearance with Sensitive Compartmented Information (SCI) eligibility

A-2 Security Assistant
Experience: Have a minimum of three years' experience in the field of security operations and worked directly in the career field during three (3) of the preceding five (5) years.
Education: High School Diploma or equivalent
Proficiencies: Possess skills/knowledge of: JPAS and/or Defense Information System for Security (DISS); security programs; inspections/self-inspections; implementing physical security safeguards; policy and procedures for handling, storing, and granting personnel and visitors' access to restricted records and materials; maintaining classified document accounts; National Industrial Security Program Operating Manual (NISPOM), NISPOM Supplement, and Director of Central Intelligence Directives (DCIDs). Possess working knowledge of a variety of physical security disciplines including but not limited to locks, alarms, security containers, risk-management and security countermeasures. Possess ability to identify and report inspection checklist facility-related items that are damaged, or

are in need of maintenance or repair. Ability in manage key control programs. Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.).
Qualifications: N/A
Security: Possess a Top Secret security clearance with SCI eligibility

A-3 Logistics Technician
Experience: Have a minimum of three years' experience or equivalent in the field of logistics operations and worked directly in the career field during three (3) of the preceding five (5) years.
Education: High School Diploma or equivalent
Proficiencies: Experience with the Supply Discipline Programs providing 100% inventory control to all items identified on the installation property book. Experience in equipment maintenance processes and procedures. Knowledge in supply policies and procedures regarding property inventories, cataloging, maintenance, transfer, and turn-in. Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.).
Qualifications: N/A
Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with SCI eligibility based on program requirements as defined in specific Task Orders.

A-4 Technical Writer
Experience: Have a minimum of three years' experience or equivalent in the field of technical writing/documentation with the US Federal Government and worked directly in the career field during three (3) of the preceding five (5) years.
Education: Undergraduate degree in a related technical discipline from an accredited institution
Proficiencies: Have the ability to effectively describe technically complex material to a non-technical audience; excellent oral and written communication skills; possess the ability to work effectively within a collaborative writing environment. Experience with project coordination and/or project scheduling. Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
Qualifications: N/A
Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with SCI eligibility based on program requirements as defined in specific Task Orders.

A-5 Operations Management Technician/Analyst
Experience:
- Documented experience in at least one of the following two areas: (1) as a branch or division leader in G3/S3 section of service headquarters (or civilian equivalent); or (2) as an Army brigade or above (or Joint service equivalent) staff officer

- A minimum of five (5) years' experience in the Army or Joint Operations Process.

Education: Undergraduate degree from an accredited institution.
Proficiencies:

- Ability to consolidate, coordinate, and track operational tasks and events.
- Knowledge of timekeeping processes and systems
- Ability to organize and maintain files to include ensuring security of sensitive and classified documents.
- Have the ability to manage a large workload and adapt to reprioritization as dictated by Government leads.
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge of the Army/Joint Operations Process
- Ability to conduct project coordination and/or project scheduling.
- Ability to track, consolidate, and present operational information.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with SCI eligibility based on program requirements as defined in specific Task Orders.

A-6 Operations Management Technician/Analyst (Unit Engagement)
Experience:

- Documented experience in at least one of the following two areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer/Non-Commissioned Officer
- A minimum of five (5) years' experience in the Army or Joint Operations Process.

Education: Undergraduate degree from an accredited institution.
Proficiencies:

- Possess at least five (5) years of relevant experience supporting Brigade, Division, or Corps Networking and operations.
- Possess current and relevant knowledge of unit structure, locations, and contacts with the ability to act as a liaison and coordinator for modernization activities.
- Ability to organize and maintain files to include ensuring security of sensitive and classified documents.
- Have the ability to manage a large workload and adapt to reprioritization as dictated by Government leads.
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities. Knowledge of the Army/Joint Operations Process
- Ability to conduct project coordination and/or project scheduling.

- Ability to track, consolidate, and present operational information
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance.

A-7 Administrative Support Technician
Experience: A minimum of one (1) year experience with Human Resources, Resourcing, Travel, Training, or Personnel Management processes
Education: High School Diploma or equivalent
Proficiencies:

- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Knowledge of Defense Travel System (DTS) including applicable regulations and policies
- Knowledge of timekeeping processes and systems
- Knowledge of training requirements and tracking systems

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance.

A-8 Executive Assistant
Experience: A minimum of three (3) years' managing incoming and outgoing correspondence, providing technical assistance to clerical staff regarding correspondence, protocol, general office management, filing, and routing incoming correspondence to appropriate staff section for action and establishing priorities.
Education: High School Diploma or equivalent
Proficiencies:

- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, etc.)
- Knowledge of Defense Travel System (DTS) including applicable regulations and policies
- Ability to manage individual and organization calendars
- Ability to receive visitors and telephone calls and relay messages in accordance with office policy
- Knowledge of timekeeping processes and systems
- Ability to organize and maintain files to include ensuring security of sensitive and classified documents.

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance.

A-9 Knowledge Manager
Experience: A minimum of (5) years' in Knowledge Management Operations.
Education: Undergraduate degree from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of Army/Joint Knowledge Management Operations Doctrine
- Knowledge of the Army/Joint Operations Process
- Knowledge of process, organizational structure, and knowledge sharing tool design
- Ability to assess, design, develop, pilot, and implement knowledge management solutions.
- Skills and ability to align people, processes, and technology to facilitate the transfer of knowledge between and among individuals and organizations
- Skills in Collaboration Services, e.g., Adobe Connect Server, Chat Services, SharePoint Portal, Electronic Email (Exchange) Server.
- Skills with Department of Defense Knowledge Management tools, e.g. InteLink and MilSuite.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with SCI eligibility based on program requirements as defined in specific Task Orders.

A-10 Systems Administrator
Experience: A minimum of five (5) years' experience administrating networks and systems, worked directly in the career field during five (5) of the preceding eight (8) years.
Education: High School Diploma or equivalent
Proficiencies: Must possess advanced IT administrator skills in remote administration, remote desktop, Group Policy Object (GPO) management, system backup and recovery, and monitor servers for performance evaluation and optimization. Must possess advanced IT Administrator skills in Collaboration Services, e.g., Adobe Connect Server, Chat Services, SharePoint Portal, Electronic Email (Exchange) Server. Must possess advance skills in datacenter management, Cloud Services, virtualization, storage area networks (SANs), data/system backups, and asset management. Must possess expert remote troubleshooting and customer service skills
Qualifications:

- This position is designated as IAWF Information Assurance Technical Level II (IAT II). Baseline certification: upon start must already possess (and maintain) current CCNA Security (preferred), GSEC, GICSP, Security+, CE, or SSCP.

Security: Obtain and Maintain a Top Secret security clearance with SCI eligibility.

A-11 Digital Graphics Designer/Print Production Specialist
Experience: A minimum of two (2) years of related technical experience with a minimum of two (2) years' experience in military operations.
Education: Undergraduate degree in Graphic Design or comparable relevant experience well

Proficiencies: Knowledge of commercial graphics design and publication software suites. Ability to visualize and develop digital representations of complex ideas/systems conveying intended message to a wide audiences. Proficiency with Microsoft Office (Word, Excel & Outlook). Ability to work both independently and as a member of a team, from concept to completion. Ability to produce high quality, professional files that are print and web ready to develop a deep understanding of the brand, audience, and key messaging.
Qualifications: N/A
Security: Obtain and Maintain a Top Secret security clearance with SCI eligibility.

A-12 Information Assurance Network Officer (IANO)
Experience:
- Possess at least five (5) years of relevant experience and extensive knowledge and understanding of network architecture and IT technology.

Education: Undergraduate degree from an accredited institution in Electrical Engineering, Computer Science, or related field.
Proficiencies:
- Ability to design and integrate network, telecommunication, and IT equipment into functional systems following all applicable standards.
- Knowledgeable of and have experience supporting DoD systems accreditation, certification, and authorization processes (e.g. DIACAP, RMF).
- Skilled in assessing & mitigating risk in information systems; performing compliance auditing of information systems; developing and maintaining DoD information systems accreditation documentation; coordinating & leading configuration control board activities.
- Exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Have the ability to manage a large workload and adapt to reprioritization as dictated by Government leads.

Qualifications: Proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—
- DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and (b) Appropriate operating system certification for information assurance technical positions as required by DOD 8570.01-M.
- Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.
- Contractor personnel who do not have proper and current certifications shall be denied access to DOD information systems for the purpose of performing information assurance functions.

Security: Obtain and Maintain a Top Secret security clearance with SCI eligibility.

A-13 DOTMLPF Capability Evaluator
Experience: A minimum of three (3) years' experience in at least one of the following two areas: (1) as an action officer in the defense acquisition community; or (2) as an action officer in a capability development position
A minimum of three (3) years' experience with training exercise development, experimentation, and testing.
Education: Undergraduate degree or equivalent job experience.
Proficiencies:
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Knowledge of Defense Acquisition System and DoD Instruction 5000.02, "Operation of the Defense Acquisition System"
- Knowledge of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H, "Operation of the JCIDS"
- Knowledge of Army/Joint Doctrine Development, Force Design, Materiel Development, Basis of Issue, Sustainment, Training/Leader Education, Personnel/Branch Proponent, and Force Modernization Proponent processes.
- Ability to develop test criteria, collect results, compile findings, and present to senior leadership orally or in writing.

Qualifications: n/a
Security: Obtain and maintain a Secret security clearance.

A-14 Concept Editor
Experience:
- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer; (3) as an assistant program manager in the defense acquisition community; or (4) as a branch or division leader in a capability development position.
- A minimum of three (3) years' experience in Army/Joint military operations and three (3) years' experience with concept development and approval processes, totaling six (6) years.

Education: Graduate degree from an accredited college or university.
Proficiencies:
- Knowledge of Joint and service organizations and their functions
- Knowledge of Army/Joint and Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:
- Military Service Intermediate Level Education; Senior Service College is preferred.

- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance.

A-15 Concept Developer

Experience:

- A minimum of three (3) years' experience in at least one of the following two areas: (1) as an action officer in the defense acquisition community; or (3) as an action officer in a capability development position
- A minimum of three (3) years' experience in Army/Joint military operations and three (3) years' experience with concept development and approval processes.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education; Senior Service College is preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance.

A-16 Scenario Developer

Experience:

- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer; (3) as an assistant program manager in the defense acquisition community; or (4) as a branch or division leader in a capability development position.
- A minimum of three (6) years' experience in Army/Joint military operations and three (3) years' experience with developing multi-threat, multi-force operational scenarios for exercise and analysis totaling (9) years.

Education: Undergraduate degree from an accredited college or university.

Proficiencies:

- Knowledge of Operational Employment of Army and Joint Force Capabilities with focus on Signal, Cyber, Electronic Warfare, and Information Related Capabilities.
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal/Cyber/Information related Army/Joint Doctrine and policies
- Knowledge of Military and Joint decision making process (e.g.,MDMP), Army/Joint Targeting process, and Intelligence cycle
- Knowledge of Validated Online Lifecycle Threat (VOLT) reporting processes and products
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education; Senior Service College is preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with SCI eligibility based on program requirements as defined in specific Task Orders.

A-17 Communications Requirements Editor

Experience:

- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer (command select list or central board selected optional but preferred); (3) as an assistant program manager in the defense acquisition community; or (4) as a branch or division leader in a capability development position.
- A minimum of three (3) years' experience in Signal Operations and three (3) years' experience with requirements and capability development documentation and approval processes, totaling six (6) years.

Education: Graduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format

- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education; Senior Service College or civilian equivalent is preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with SCI eligibility based on program requirements as defined in specific Task Orders.

A-18 Communications Requirements Editor (Architecture)

Experience:

- Must have at least two (2) years' experience in the development of Army Architectures supporting Army Networks
- Possess at least ten (10) years' experience with army military equipment in tactical operating environments.
- Possess two (2) years of relevant experience in development of data models from both program level and enterprise level views.
- A minimum of three (3) years' experience in Signal Operations and Signal Force Structure.
- Experience with the staffing and approval of capability requirements document through the Army Requirements Oversight Council (AROC) or Joint Requirements Oversight Council (JROC).

Education: Graduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:

- Knowledge of Army and Joint Multi-Domain Operations concepts and applicable technologies.
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.
- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education or equivalent; Senior Staff Course or Senior Service College is preferred.

- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements as defined in specific Task Orders.

A-19 Communications Requirements Editor (Test & Evaluation)
Experience:

- A minimum of three (3) years' experience in performing and executing operational tests and evaluations.
- Experience in writing Critical Operational Issues and Criteria (COICs) and Test Evaluation Master Plans (TEMPs).
- Experience with the staffing and approval of capability requirements document through the Army Requirements Oversight Council (AROC) or Joint Requirements Oversight Council (JROC).

Education: Graduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.
Proficiencies:

- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.
- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.
Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-20 Communications Requirements Editor (Integration)
Experience:

- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army

division or above (or Joint service equivalent) staff officer; or (3) as a branch or division leader in a capability development position.
- A minimum of three (3) years' experience in Signal Operations and Signal Force Structure.
- Experience with the staffing and approval of capability requirements document through the Army Requirements Oversight Council (AROC) or Joint Requirements Oversight Council (JROC).

Education: Graduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:
- Knowledge of Army and Joint Multi-Domain Operations concepts and applicable technologies.
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.
- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:
- Military Service Intermediate Level Education or equivalent; Senior Staff Course or Senior Service College is preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-21 Communications Requirements Editor (SATCOM Systems Analyst)

Experience:
- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer; or (3) as a branch or division leader in a capability development position.
- Experience in Signal Operations and Signal Force Structure.
- Experience with the staffing and approval of capability requirements document through the Army Requirements Oversight Council (AROC) or Joint Requirements Oversight Council (JROC).

- Possess minimum of 15 Years' experience in DOD communications and/or satellite communications.
- Have at least 10 years experience with military and commercial SATCOM systems including AEHF, WGS, DCS, UFO, EMI and jamming as well as expertise with DOD ground and airborne SATCOM terminals.
- (Optional – preferred) Possess 10 years experience with EHF and AEHF satellite communications and how it interfaces with the Navy, Missile Defense Command, and Air Force.

Education: Graduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:

- Have the ability to provide technical expertise in the design and development of enterprise transport solutions.
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Have the ability to manage a large workload and adapt to reprioritization as dictated by Government leads.
- Knowledge of Army and Joint Multi-Domain Operations concepts and applicable technologies.
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- (Optional – preferred) Military Service Intermediate Level Education or equivalent; Senior Staff Course or Senior Service College is preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-22 Cyberspace Operations Requirements Editor

Experience:

- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer (command select list or central board selected optional but preferred); (3) as an assistant program manager in the defense acquisition community; or (4) as a branch or division leader in a capability development position.
- A minimum of three (3) years' experience in operational Cyberspace Operations and three (3) years' experience with requirements and capability development documentation and approval processes, totaling six (6) years.

Education: Graduate degree in Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service Cyberspace Operations organizations and their functions
- Knowledge of Cyberspace Operations related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education; Senior Service College or civilian equivalent is preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-23 Electromagnetic Spectrum Operations (EMSO) Requirements Editor

Experience:

- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer (command select list or central board selected optional but preferred); (3) as an assistant program manager in the defense acquisition community; or (4) as a branch or division leader in a capability development position.
- A minimum of three (3) years' experience in operational electronic warfare or spectrum management and three (3) years' experience with requirements and capability development documentation and approval processes, totaling six (6) years.
  - **Education:** Graduate degree with a preference for major in Electrical Engineering, Physics, Engineering, Telecommunications Management, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service EMSO organizations and their functions
- Knowledge of EMSO related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education; Senior Service College or civilian equivalent is preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-24 Information Related Capabilities Requirement Editor

Experience:

- Documented experience in at least one of the following four areas: (1) as a branch or division leader at the Service headquarters level; or (2) as an Army division or above (or Joint service equivalent) staff officer (command select list or central board selected optional but preferred); (3) as an assistant program manager in the defense acquisition community; or (4) as a branch or division leader in a capability development position.
- A minimum of three (3) years' experience in Information Operations, Psychological Operations/ Military Information Support Operations (MISO), Civil Affairs, and/or Special Operations and three (3) years' experience with requirements and capability development documentation and approval processes, totaling six (6) years.

Education: Master's Degree from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service Information Operations, Psychological Operations/ Military Information Support Operations (MISO), Civil Affairs, and Special Operations organizations and their functions
- Knowledge of Information Operations, Psychological Operations/ Military Information Support Operations (MISO), Civil Affairs, and Special Operations related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education; Senior Service College or civilian equivalent is preferred.

- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-25 Communications Requirements Developer

Experience:

- A minimum of three (3) years' experience in at least one of the following two areas: (1) as an action officer in the defense acquisition community; or (2) as an action officer in a capability development position
- A minimum of three (3) years' experience with requirements and capability development documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education or civilian equivalent; Senior Service College or civilian equivalent is optional but preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-26 Communications Requirements Developer (Tactical Transport)

Experience:

- A minimum of two (2) years' experience with requirements development, documentation and approval processes

- A minimum of two (2) years' experience with commercial wireless technologies (4G/5G, cellular, 802.x wireless, MIMO, broadband, multichannel wireless systems, etc.)
- A minimum of two (2) years' experience with beyond line of site transport systems (e.g. TROPO)
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- (Optional – preferred) Experience working with Department of Homeland Security (DHS) in support of civil authority missions

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-27 Communications Requirements Developer (Tactical Network)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- A minimum of three (3) years' experience with network technologies (e.g. routing, switching, point-to-point and point-to-multipoint transmission systems, etc.)
- Experience in the installation, configuration, and management of voice communication technologies and architectures (e.g. CUCM, Unified Communications, REDCOM, etc.)
- A minimum of three (3) years' experience in Signal Operations

- (Optional – preferred) Experience working with Department of Homeland Security (DHS) in support of civil authority missions

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of Army Line of Sight communications and Tropospheric Scatter systems.
- Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-28 Communications Requirements Developer (Tactical SATCOM)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- A minimum of five (5) years' experience or equivalent in tactical SATCOM terminals. This includes experience providing centralized network operations and management to include the preparation and processing of Satellite Access Requests and Alternate Satellite Requests.
- Possess minimum of 5 Years' experience in DOD satellite communications and/or commercial satellite communications.
- (Optional – preferred) Must have at least 5 years experience with SATCOM systems including AEHF, WGS, DCS, UFO, EMI and jamming as well as expertise with DoD ground or airborne SATCOM terminals.

- (Optional – preferred) Must have experience with protected SATCOM systems and technology.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of emerging tactical SATCOM communications technologies
- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-29 Communications Requirements Developer (Enterprise Transport)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- A minimum of two (2) years' experience with commercial network transport technologies (Land Mobile Radio, First Responder Radio Networks, Public Safety FM Networks, Army Tech Control Facilities, Installation Network Infrastructure, Installation Processing Nodes, Special Processing Nodes, etc.)
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- (Optional – preferred) Experience working with Department of Homeland Security (DHS) in support of civil authority missions

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- (Optional – preferred) Knowledge of JCIDS
- Knowledge of Army Base/Post/Camp/Station (BPCS) enterprise information technology facilities and network infrastructure.
- Have the ability to provide technical expertise in the design and development of enterprise transport solutions.
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications:

- (Optional – preferred) Trained on the national Program 25 (P25) interoperability standard.
- Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-30 Communications Requirements Developer (Enterprise DoDIN Ops)
Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- A minimum of three (3) years' experience managing, securing, and monitoring Army Enterprise level networks (e.g. NEC, RCC, ACOIC, or ARCYBER Network Operations centers); commercial equivalent accepted based upon approval by the COR
- Experience with the configuration and management of Enterprise level Network Operations tools (e.g. Tanium, IBM Tivoli, CA Unicenter, Microsoft Systems Center, Arcsight, Remedy, etc.)
- Experience with the coordination and reporting from subordinate network operations centers.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university.

Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of the Virtual Machine technologies
- Knowledge of routing and switching network technologies
- (Optional – preferred) Knowledge of Cyber Security tools/technologies
- (Optional – preferred) Knowledge of Information Dissemination Management/Content Staging (IDM/CS) technologies
- Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- (Optional – preferred) Knowledge of implementing ITILv3 best practices for managing information technology (IT)
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-31 Communications Requirements Developer (Tactical DoDIN Ops)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- A minimum of three (3) years' experience in Signal Operations
- A minimum of three (3) years' experience managing, securing, and monitoring Army Tactical level networks (e.g. BCT, Division, Corps, Joint, etc.)
- Experience with the configuration and management of Tactical level Network Operations tools (e.g. SNMPC, NMS, Microsoft Systems Center, Solarwinds Orion, NOMS, PACSTAR, etc.)
- Experience with the coordination and reporting to and from higher or lower network operations centers.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university.

Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of the Virtual Machine technologies
- Knowledge of routing and switching network technologies
- (Optional – preferred) Knowledge of Cyber Security tools/technologies
- (Optional – preferred) Knowledge of Information Dissemination Management/Content Staging (IDM/CS) technologies
- Knowledge of JCIDS
- Knowledge of Army/Joint organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- (Optional – preferred) Knowledge of implementing ITILv3 best practices for managing information technology (IT)
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-32 Communications Requirements Developer (Cyber Security)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- A minimum of three (3) years' experience securing tactical and/or enterprise networks and services (e.g. BCT, Division, Corps, Joint, NEC, RCC, ACOIC, or ARCYBER Network Operations centers); commercial equivalent accepted based upon approval by the COR
- Experience with the configuration and management of cyber security tools and infrastructure (e.g. SIEM, HBSS, Tanium, Microsoft Systems Center, Arcsight, Splunk, Security Onion, Panorama, Security Center, PKI, etc.)
- Experience with the coordination and reporting security events to and from higher or lower network operations centers.

Education: Undergraduate degree in Cyber Security, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university.

Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- (Optional – preferred) Knowledge of the Virtual Machine technologies
- (Optional – preferred) Knowledge of routing and switching network technologies
- Knowledge of Cyber Security tools/technologies
- (Optional – preferred) Knowledge of Information Dissemination Management/Content Staging (IDM/CS) technologies
- (Optional – preferred) Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- (Optional – preferred) Knowledge of implementing ITILv3 best practices for managing information technology (IT)
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications:

- Within six (6) months from the beginning of the contract the contractor must obtain a Certified Information Security System Professional (CISSP) and/or Security Plus/Network Plus Certification. Equivalent undergraduate education or certifications may be accepted by the COR.
- Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-33 Communications Requirements Developer (COMSEC/KMI)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- Have at least three (3) years of experience with Army COMSEC/KMI tools and system (AKMS, Army Fill Devices, COMSEC, Network Defense capabilities, etc.)
- A minimum of three (3) years' experience in Signal Operations
- Experience with the request, distribution, and security of COMSEC material.

Education: Undergraduate degree in Cyber Security, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of COMSEC mission planning and execution.
- Knowledge of COMSEC policy and procedures.
- Knowledge of JCIDS
- Knowledge of Army/Joint organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications:

- Within six (6) months from the beginning of the contract the contractor must obtain a Certified Information Security System Professional (CISSP) and/or Security Plus/Network Plus Certification. Equivalent undergraduate education or certifications may be accepted by the COR.
- Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-34 Communications Requirements Developer (IDM/CS)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- A minimum of three (3) years' experience in Signal Operations
- A minimum of three (3) years' experience providing IDM/CS and data recovery services at the tactical and/or enterprise level (e.g. BCT, Division, Corps, Joint, NEC, RCC, ACOIC, or ARCYBER Network Operations centers); commercial equivalent accepted based upon approval by the COR
- Experience with the configuration and management of content/recovery tools and storage (e.g. SharePoint, VMWare, databases, storage infrastructure, etc.)
- Experience with the coordination and reporting to and from higher or lower network operations centers.

Education: Undergraduate degree in Data Science, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of the Virtual Machine technologies
- Knowledge of data discovery, delivery, storage, and recovery technologies
- Knowledge of data contingency of operations planning (COOP)
- Knowledge of Information Dissemination Management/Content Staging (IDM/CS) technologies; commercial equivalent accepted based upon approval by the COR
- (Optional – preferred) Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-35 Communications Requirements Developer (Enterprise Data/Cloud)

Experience:

- A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- A minimum of two (2) years' experience with the operations and installation of commercial cloud and storage technologies (AWS, Microsoft AZURE, VMWARE infrastructure, etc.). Education/certification may be substituted for experience.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university.

Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- (Optional – preferred) Knowledge of implementing ITILv3 best practices for managing information technology (IT)
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-36 Communications Requirements Developer (Enterprise Services Infrastructure)

Experience:

- A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- A minimum of two (3) years' experience with the operations and installation of commercial services, servers, and data storage and infrastructure technologies. Education/certification may be substituted for experience.
- A minimum of two (3) years' experience with virtual machine, server, and operating system technologies (e.g. VMWare, Microsoft Virtual Server, Virtual Box, etc.) (Experience may be concurrent with infrastructure experience).

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS

- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- (Optional – preferred) Knowledge of implementing ITILv3 best practices for managing information technology (IT)
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-37 Communications Requirements Developer (Tactical Services Infrastructure)

Experience:

- A minimum of two (2) years' experience with requirements development, documentation and approval processes
- A minimum of three (3) years' experience in Signal Operations and Signal Force Structure.
- A minimum of two (3) years' experience with the operations and installation of tactical services, servers, and data storage and infrastructure technologies.
- A minimum of two (3) years' experience with virtual machine, server, and operating system technologies (e.g. VMWare, Microsoft Virtual Server, Virtual Box, etc.) (experience may be concurrent with infrastructure experience).
- Possess at least three (3) years of relevant experience with the Battle Command Server Stack/Tactical Services Infrastructure supporting Company, Battalion, and Brigade Networking.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions

- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies
- (Optional – preferred) Knowledge of implementing ITILv3 best practices for managing information technology (IT)
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-38 Communications Requirements Developer (Enterprise Computing Environment)

Experience:

- A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- A minimum of two (3) years' experience with software development and application development lifecycle. Education/certification may be substituted for experience.
- Experience in deploying and managing Business Mission Area (BMA), Enterprise Resource Management (ERP), or cloud based applications.
- A minimum of two (3) years' experience with virtual machine, server, and operating system technologies (e.g. VMWare, Microsoft Virtual Server, Virtual Box, etc.) (Experience may be concurrent with infrastructure experience).

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies

- (Optional – preferred) Knowledge of implementing ITILv3 best practices for managing information technology (IT)
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications:

- (Optional – preferred) Cloud based certification with a focus on application development or content delivery.
- Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-39 Communications Requirements Developer (Mission Partner Interoperability)

Experience:

- A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- (Optional – preferred) Possess at least two (2) years of relevant experience working with network and services integration or standards development (e.g. ABCANZ/FVEY, NATO, FMN, etc.)
- A minimum of two (3) years' experience in coordination, developing, and executing unified action partner network and services integration.
- Experience with coalition interoperability at the Corps, Division, or Joint level.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- (Optional – preferred) Knowledge of Army/Joint organizations and their functions
- (Optional – preferred) Knowledge of Signal related Army/Joint Doctrine and policies

- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-40 Communications Requirements Developer (Enterprise Network)

Experience:

- Possess at least five (5) years of relevant experience and extensive knowledge and understanding of network architecture and IT technology to include routing, switching, voice, and data transfer.
- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- Experience in Signal Operations and Signal Force Structure.
- Possess minimum of three (3) years' experience working with enterprise gateways (e.g. THN, RHN, Step Sites, Teleport, etc.)

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Have the ability to provide technical expertise in the design and development of enterprise transport solutions.
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Have the ability to manage a large workload and adapt to reprioritization as dictated by Government leads.
- Knowledge of Army and Joint Multi-Domain Operations concepts and applicable technologies.
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Knowledge of the enterprise network administration and procedures.

- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications:

- Must have certification and provide verification of Cisco Certified Network Associate (CCNA) or equivalent. All required certifications must be maintained and updated as needed. Equivalent undergraduate education or certifications may be accepted by the COR.
- Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first 30 days of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-41 Communications Requirements Developer (Enterprise SATCOM)

Experience:

- (Optional – preferred) A minimum of two (2) years' experience with requirements development, documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Signal Operations
- A minimum of ten (10) years' experience or equivalent in systems engineering enterprise SATCOM terminals. This includes experience providing centralized network operations and management to include the planning, preparation, processing, and resourcing of Satellite Requests.
- Possess minimum of 5 Years' experience in DOD satellite communications and/or commercial satellite communications.
- (Optional – preferred) Must have at least 5 years experience with SATCOM systems including AEHF, WGS, DCS, UFO, EMI and jamming as well as expertise with DoD ground and airborne SATCOM terminals.
- Must have experience with protected SATCOM systems and technology.

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of emerging enterprise/commercial SATCOM communications technologies
- Knowledge of JCIDS

- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Have exceptional written and verbal communications skills, briefing skills, and the ability to work closely with a wide range of DOD and other contractor entities.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Have the ability to work within a team, manage a large workload, and adapt to reprioritization as dictated by Government leads.

Qualifications: Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-42 Communications Requirements Developer (LNO)

Experience:

- (Optional – preferred) A minimum of three (3) years' experience in at least one of the following two areas: (1) as an action officer in the defense acquisition community; or (2) as an action officer in a capability development position
- (Optional – preferred) A minimum of three (3) years' experience with requirements and capability development documentation and approval processes
- A minimum of three (3) years' experience in Signal Operations

Education: Undergraduate degree in Electrical Engineering, Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service Signal/Communications organizations and their functions
- Knowledge of Signal related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education; Senior Service College is preferred.
- Shall complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-43 Cyberspace Operations Requirements Developer
Experience:
- A minimum of three (3) years' experience in at least one of the following two areas: (1) as an action officer in the defense acquisition community; or (2) as an action officer in a capability development position
- A minimum of three (3) years' experience with requirements and capability development documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in Cyberspace Operations

Education: Undergraduate degree in Computer Science, Information Systems Management, Networking, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.
Proficiencies:
- Knowledge of JCIDS
- Knowledge of Joint and service Cyberspace Operations organizations and their functions
- Knowledge of Cyberspace Operations related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:
- Military Service Intermediate Level Education or civilian equivalent; Senior Service College or civilian equivalent is optional but preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-44 Electromagnetic Spectrum Operations (EMSO) Requirements Developer
Experience:
- A minimum of three (3) years' experience in at least one of the following three areas: (1) as an action officer in the defense acquisition community; (2) as an action officer in a capability development position; or as an action officer at the Service headquarters-level.
- A minimum of three (3) years' experience with requirements and capability development documentation and approval processes
- (Optional – preferred) A minimum of three (3) years' experience in EMSO

Education: Undergraduate degree with a preference for major in Electrical Engineering, Physics, Engineering, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service EMSO organizations and their functions
- Knowledge of EMSO related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education or civilian equivalent; Senior Service College or civilian equivalent is optional but preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-45 Electromagnetic Spectrum Operations (EMSO) Requirement Developer (Junior):

Experience:

- Experience in at least one of the following three areas: (1) as an electronic warfare or spectrum management staff position at corps or below; or (2) as an action officer in the defense acquisition community; or (3) as an action officer in a capability development position
- Three or more years' experience in electronic warfare or spectrum management in tactical organizations
- One year experience in requirements and capability development, documentation, and approval processes

Education: Associate degree with a preference for a major in Electrical Engineering, any engineering, physics, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service EMSO organizations and their functions
- Knowledge of EMSO related Army/Joint Doctrine and policies
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Former military primary occupation in electronic warfare or spectrum management, or civilian equivalent.

- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-46 Electromagnetic Spectrum Operations (EMSO) Requirements Developer (Operations Support)

Experience:

- Experience in at least one of the following three areas: (1) as an administrative center supervisor; (2) as an adjutant officer at battalion or above; or (3) as an action officer in a capability development position, responsible for coordinating and facilitating office meetings, teleconferences, VTCs, and similar events
- Experience editing documents for grammar, format, clarity, clarity, and logical information content.
- Experience in knowledge management
- Experience in physical security policy and procedures

Education: Undergraduate degree with a preference for a major in Electrical Engineering, any engineering, physics, Telecommunications Management, or related technical field from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service EMSO organizations and their functions
- Knowledge of EMSO related Army/Joint Doctrine and policies
- Knowledge management technology and processes
- Knowledge of physical security policy and procedures
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education or civilian equivalent.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-47 Information Related Capabilities Requirement Developer

Experience:

- A minimum of three (3) years' experience in at least one of the following two areas: (1) as an action officer in the defense acquisition community; or (2) as an action officer in a capability development position
- A minimum of three (3) years' experience with requirements and capability development documentation and approval processes

- A minimum of three (3) years' experience in Information Operations, Psychological Operations/Military Information Support Operations (MISO), Civil Affairs, Public Affairs, and Military Deception, and/or Operations Security.

Education: Undergraduate degree from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.

Proficiencies:

- Knowledge of JCIDS
- Knowledge of Joint and service Information Operations, Psychological Operations/Military Information Support Operations (MISO), Civil Affairs, Public Affairs, and Military Deception, and/or Operations Security organizations, functions, doctrine, and policies.
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications:

- Military Service Intermediate Level Education or civilian equivalent; Senior Service College or civilian equivalent is optional but preferred.
- Will complete Defense Acquisition University online courses CLR 101 Introduction to JCIDS, and RQM 110 Core Concepts for Requirements Management within the first two weeks of employment.

Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-48 Operations Research and Systems Analyst

Experience: A minimum of three (3) years' experience as an Operations Research/Systems Analyst (preferred as Army Functional Area 49)

Education: Graduate degree in mathematics, operations research, statistics, computer science, management science, physics, or related technical field from an accredited college or university. Undergraduate degree may be accepted as determined by the COR.

Proficiencies:

- Skill in applying and documenting the results of advanced decision-support techniques from mathematics, science, and engineering.
- Ability to use sophisticated computer software, such as databases and statistical and modeling packages, to analyze and solve problems.
- Knowledge of Army and Joint Signal, Cyberspace Operations, Electronic Warfare, and Information Environment Operations.

Qualifications: N/A

Security: Obtain and maintain a Secret security clearance.

A-49 Capability Cost Analyst

Experience: A minimum of three (3) years' experience in at least one of the following two areas: (1) as an action officer in the defense acquisition community; or (2) as an action officer in a capability development position
Education: Undergraduate degree from an accredited college or university. Additional experience may be accepted in lieu of degree as determined by the COR.
Proficiencies:

- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Knowledge of procedures for determining, recording, and reporting measurements of the capability and program costs in the aggregate and in detail.
- Knowledge of Cost – Benefit Analysis processes and deliverables
- Extensive Knowledge of Defense Acquisition System and DoD Instruction 5000.02, "Operation of the Defense Acquisition System"
- Extensive Knowledge of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H, "Operation of the Joint Capabilities Integration and Development System"

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance.

A-50 Modeling and Simulation Analyst
Experience:

- Must have experience with model ready data to support M&S of tactical and communications networks, cyber and EW requirements.
- Must have experience and understanding of Army force structure and force modernization efforts.
- Must have hands-on experience with tactical communications networks

Education: Undergraduate degree with minimum of 30 semester hours in a combination of mathematics, statistics, and computer science with at least 4 years' experience directly supervising and managing information technology projects.
Proficiencies: Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.). Possess advanced writing and presentation speaking skills.
Qualifications: N/A
Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-51 Communications Analyst
Experience: A minimum of five (5) years' experience in operational Signal planning, implementation, and configuration (Signal Branch/Military Occupation Specialty or Commercial Equivalent). Shall have experience in installation, operation, troubleshooting, maintenance and upgrades required to the RHN-E satellite enclave hardware, to include satellite servers, modems and facility antennas. Be knowledgeable and have a minimum of 10 years experience in the

following areas: Providing power balancing on RHN-E TDMA and FDMA networks; Configuring missions on Network Management System for TDMA network access; Frequency management and operations of MRT/Network control; COMSEC key management; Linkway network implementation by programming Network Control Console (NCC) and servers for satellite networks; Spacecraft acquisition, peak and pole antenna and controllers; Bandwidth Management to include an in depth knowledge of modems, data and symbol rates, link budgets, and satellite payload planning, with the ability to formulate future bandwidth resource requirements.
Education: Undergraduate degree in an information technology related field or equivalent job experience.
Proficiencies:

- Demonstrated ability to plan, conduct, and execute Signal Operations.
- Demonstrated knowledge of networking technologies.
- Demonstrated knowledge and understanding of performing communications network engineering, integration and operations including planning, coordinating, or evaluating actions required to support a specified mission, weapons system, or other designated program.

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-52 Cyberspace Operations Analyst
Experience: A minimum of five (5) years' prior military experience and/or significant civilian occupational experience in Cyberspace Operations (Defensive Cyberspace Operations, Offensive Cyberspace Operations, or Cyberspace Situational Awareness).
Education: Undergraduate degree in Computer Science or Computer Engineering from an accredited institution. Coursework shall include computer programming (e.g., Fundamentals of Programming, Computer Forensics) and coding (e.g., C, C++, Python, Java). Equivalent job experience may be considered.
Proficiencies: Knowledge of Cyberspace Warfare including, but not exclusively, computer programming, software design, cyber security (defensive or offensive), and cyber forensics.
Qualifications: Desired Certifications: CISSP, Global Industrial Cyber Security Professional (GICSP), GIAC Enterprise Defender (GCED), GIAC Information Security Professional (GISP).
Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-53 Electromagnetic Spectrum Operations Analyst
Experience: A minimum of five (5) years' experience in operational EW, Spectrum Management Operations, and Signals Intelligence planning,

implementation, and configuration (Military Occupation Specialties MOS 17E,25E, and 35G. or Equivalent).
Education: Undergraduate degree in Engineering, Physics, or equivalent job experience.
Proficiencies:
- Demonstrated ability to plan, conduct, and execute EW/SMO/SIGINT including the use of electromagnetic energy to determine, exploit, reduce, and prevent hostile use of the electromagnetic spectrum.
- Demonstrated knowledge of the Electromagnetic Spectrum.

Qualifications: Must possess Military or Commercial EW/SMO/SIGINT qualification upon task order start.
Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-54 Information Related Capabilities Analyst
Experience: A minimum of five (5) years' experience in planning, integrating, coordinating, and synchronizing Information Operations, Psychological Operations/Military Information Support Operations (MISO), Civil Affairs, Public Affairs, Military Deception, and Operations Security.
Education: Undergraduate degree or equivalent job experience.
Proficiencies:
- Knowledge of Joint and service Information Operations, Psychological Operations/Military Information Support Operations (MISO), Civil Affairs, Public Affairs, and Military Deception, and Operations Security organizations and their functions, policies, and related military occupational specialties and associated knowledge, skills, and abilities.
- Ability to edit documents for correct grammar and format.
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance. Anticipate specified contractors shall require Top Secret Security Clearance with Sensitive Compartmented Information (SCI) eligibility based on program requirements defined in specific Task Orders.

A-55 Data Analyst
Experience: A minimum of five (5) years' experience in data management, analytics, and visualization.
Education: Undergraduate degree from an accredited university in automated data management.
Proficiencies:
- Demonstrated ability to perform advanced data analytics.
- Knowledge of data science concepts, principles, and industry best practices.

Qualifications: N/A.
Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.

A-56 Capability Integrator
Experience: A minimum of three (3) years' experience as an action officer in developing, integrating, and submitting requirements documents IAW the Joint Capabilities Integration and Development System, Defense Acquisition System, and force management processes.
Education: Undergraduate degree or equivalent job experience.
Proficiencies:

- Ability to analyze joint and Army cyberspace, Signal, EW, and information concepts to determine associated required capabilities.
- Knowledge of wargaming, experimentation, and concepts to develop and integrate requirements from a comprehensive perspective of DOTMLPF.
- Skill to coordinate with other CDIDs and CoEs to execute the CoE functions of delivering current warfighting requirements, identifying future capabilities, integrating DOTMLPF domains, and presenting recommendations.
- Determine and integrate force requirements and synchronize the development of DOTMLPF solutions. Capture this information in capability mapping or strategic frameworks.
- Ability to analyze, design, and assess cyberspace, Signal, EW, and other information capability requirements , concepts, and resources to merge, de-conflict, and synchronize functional, organizational, and DOTMLPF capability requirements and solutions.
- Ability to participate in associated working/focus group meetings and in progress reviews.
- Ability to research, manage, analyze, and document requirements for doctrine, organizations, training, leader development and education, materiel, personnel, facilities and policy implications.
- Ability to edit documents for correct grammar and format
- Knowledge in computer automation software (have a working knowledge of Word, PowerPoint, Excel, Spreadsheets, Outlook, Outlook Calendars, etc.)
- Extensive Knowledge of Defense Acquisition System and DoD Instruction 5000.02, "Operation of the Defense Acquisition System"
- Extensive Knowledge of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H, "Operation of the Joint Capabilities Integration and Development System"
- Knowledge of Doctrine Development, Force Design, Materiel Development, Basis of Issue, Sustainment, Training/Leader Education, Personnel/Branch Proponent, and Force Modernization Proponent processes.

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance.

A-57 Force Design Developer
Experience: A minimum of three (3) years' experience developing organizational and force structure requirements.
Education: Undergraduate degree or equivalent job experience.
Proficiencies:

- Knowledge of Army and Joint Signal, Cyberspace Operations, Electronic Warfare organizations.
- Knowledge of Total Army Analysis (TAA) and force design update (FDU) processes.
- Ability to design and integrate unit designs, force structure, and TOE documentation actions to include the development of Rules of Allocation for TOEs.
- Ability to identify organizational and force structure solutions to resolve or mitigate gaps.

Qualifications: N/A
Security: Obtain and maintain a Secret security clearance.

A-58 Threat and Operational Environment Analyst
Experience: A minimum of three (3) years' experience conducting intelligence and threat support activities.
Education: Undergraduate degree or equivalent job experience.
Proficiencies:

- Ability to conduct research resulting in various reports and alerts.
- Ability to develop targeted intelligence products such as forecasts and capabilities assessments for weapon system or technology studies.
- Knowledge of Army and Joint Signal/Network, Cyberspace Operations, Electronic Warfare capabilities, Operations in the Information Environment.
- Knowledge of Validated Online Lifecycle Threat (VOLT) reporting processes and products
- Ability to collaborate throughout the Intelligence Community and customer activities to devise methods for exchange, verification, and integration of technical data.

Qualifications: N/A
Security: Obtain and maintain a Top Secret security clearance with SCI eligibility.