PERFORMANCE WORK STATEMENT (PWS)

FOR

PIONEER

1. Purpose

The purpose of this contract is to provide contract manpower equivalents in support of the 67th Cyberspace Operations Group's (67 COG) Distributed Cyber Warfare Operations (DCWO) mission. The 67 COG is the USAF's premiere cyber operations group supporting national and Combatant Command objectives and strategies.

2. Scope

This contract will entail a broad scope of specialties in order to provide unique work resident in the 67 COG units and staff. General work roles include system and platform engineering; system administration (SYSAD) and Computer Support Technicians (CST); executive, human resources and administrative support; budget analysis and resource advisors; physical, personnel, industrial, and information systems security; project and program management; software development and engineering; knowledge management; intelligence analysis, research, and collection management; training and curriculum development; military exercise planning and cyber range management; unit deployment managers and readiness reporting; and strategic and tactical planning.

3. Requirement/Description of Services. **See individual unit level PWSs and Contract Data Requirements Lists (CDRL) for specific work roles and deliverables.**

3.1 Engineering

3.1.1 The network engineers will work closely with vendors, program management offices, mission subject matter experts (SME), and others to ensure integration, interoperability, and stability of the mission infrastructure. The network engineers will be called upon to innovate and execute solutions to unique challenges presented to them as the infrastructure grows and becomes a part of a national federated enterprise. The network engineers will keep track of status of patches, improvement, development operations, system performance, and write/track requirements pertaining to the mission systems.

3.1.2 Requires DOD Directive 8570.01 IA Baseline Certification Requirement for IAT Level II in order to enable elevated privileges. See the IA Baseline Certification Requirements table for IAT Level II at: https://www.imgva.com/8570-requirements.

3.1.3 Required training: Linux+, NET+, Firewall configuration, Red Hat. Must be familiar with the following software: Juniper, PFSense, OpenNebula, Elastic Kibana, Zentayl, FreeIPA.

3.1.4 Deliverables will include engineering designs, project objectives and milestone (POAM) plans, briefing, trip reports, and meeting minutes.

3.2 System Administration/Computer Support Technician

3.2.1 The contractors shall provide on-site, day-to-day assistance with maintaining unit mission systems, cloud services and subsystems IAW Air Force and Joint IT standards; coordinate timely resolution of and follow-up on software and hardware problems with all levels of IT resources including network, server, and application operations; troubleshoot and diagnose, maintain, service, and repair computer hardware, peripherals, and software; provide individual, hands-on training to users on request; provide network accounts and passwords as required; maintain current and accurate inventory of technology hardware, software and resources; and perform related duties as assigned.

3.2.2 The contractors will serve as mission system auditors as required. The contractors shall ensure stored material confidence and protection IAW Air Force and Joint standards to include back-ups, file plans, naming conventions, and storage; monitor security of all technology; audit systems and report status; preserve information security, safeguard backups and other sensitive data. The contractors may be asked to troubleshoot VTC systems, perform basic network infrastructure services, or oversee IT projects as necessary.

3.2.3 Requires DOD Directive 8570.01 IA Baseline Certification Requirement for IAT Level II in order to enable elevated privileges. See the IA Baseline Certification Requirements table for IAT Level II at: https://www.imgva.com/8570-requirements.

3.3.4 Some positions will require cloud services training and certifications including Amazon Web Services (AWS) Advanced Developing on AWS, Advanced Developing on AWS, Advanced Developing on AWS, Advanced Developing on AWS, Advanced Developing on AWS, Advanced Developing on AWS, Advanced Developing on AWS, and Migrating to AWS.

3.2.5 Deliverables will include engineering designs, project objectives and milestone (POAM) plans, briefing, trip reports, and meeting minutes.

3.3 Executive, Human Resources, and Administrative Support

3.3.1 The contractor shall provide executive services including maintaining unit leadership calendars and schedules, organizing commander's calls and other official events, reviewing and editing correspondence, tracking staff actions, and prepare for distinguished visitors.

3.3.2 The contractor shall provide human resources support including preparation of civilian and military hiring actions, maintaining unit manpower documents (UMD) and rosters, update duty status, and ensuring recall rosters are up to date.

3.3.3 The contractor shall provide administrative support by accessing and utilizing various military and civilian personnel and administrative systems such as Virtual Military Personnel Flight (vMPF), Base Level Service Delivery Model (BLSDM), MyPers, Defense Civilian

Personnel System (DCPS, AKA "MyBiz+), Virtual Processing Center (vPC), Personnel Records Display Application (PRDA), Case Management System (CMS), LeaveWeb, SharePoint, Military Personnel Data System (MilPDS), Automated Time Attendance and Production System (ATAAPS), Air Force Personnel Accountability and Assessment System (AFPAAS), the Defense Travel System (DTS).

3.3.4 Deliverables will include briefings, staff action tracking reports, and programs for official events.

3.4 Budget Analysis and Resource Advisors

3.4.1 The contractor shall perform and conduct data collection and analysis, including business case analysis, Analysis of Alternatives (AoA), cost-benefit analysis, financial impact analysis, government budget planning, expenditure tracking and reconciliation, cost allocation, and cost recovery, analyzing multiple data sources to generate strategic fiscal planning reports for command staff. The contractor shall: analyze multiple data sources to generate strategic fiscal planning reports for leadership; operate and improve existing tools and models, build new financial models to analyze and reconcile program data plus forecast over the Fiscal Year Defense Program (FYDP), and develop program reports and recommendations for improvements regarding the overall budget and execution process and strategic reporting capabilities; prepare briefings and reports for leadership to summarize estimates, findings, cost-benefit analysis and recommend best course of action. The Contractor shall identify and define requirements and resources for Planning, Programming, Budgeting, and Execution (PPBE) process to meet unit strategic goals. This requirement includes identifying future needs and matching those needs with corresponding fund types for resourcing in the areas of: manpower, IT, travel, training and annual supply needs. The contractor shall document the requirements and associated information in Government approved formats. The contractor shall maintain these documents in an appropriate electronic Government approved shared location.

3.4.2 Deliverables will include budget and spend plans, briefings, meeting minutes, and financial planning documents as described in paragraph 3.4.1.

3.5 Physical, Personnel, Industrial, and Information Systems Security

3.5.1 Personnel Security: The contractor shall administer unit-level Special Access Programs (SAP). The Activity Security Representative's primary function is to provide multi-disciplined security support to a customer's facility and organization. The position will provide "day-to-day" support for Collateral, Sensitive Compartmented Information (SCI) and Special Access Program (SAP) activities. Must be able to use Joint Personnel Access System (JPAS) and other security databases. Must complete DoD SAP Nomination Process training. Will develop and present security training.

3.5.2 Physical (Area and Facility) Security: The contractor shall ensure facilities meet National Security Agency (NSA), Defense Intelligence Agency (DIA), and HQ Air Force SAP standards.

3.5.3 Information Systems Security: The contractor shall perform Information Systems Security Officer (ISSO) and Information Systems Security Manger (ISSM) duties and perform Risk Management Framework (RMF) to attain and maintain Authority to Operate (ATO) and Authority to Connect (ATC).

3.5.4 Industrial Security: The contractor shall coordinate with Cleared Defense Contractor (CDC) companies to process necessary accesses for contract personnel.

3.5.5 Deliverables will include security review determinations, security training materials, status reports, RMF packages, briefings, and meeting minutes.

3.6 Project Management

3.6.1 Project Management: The contractor shall manage projects which may include facilities, cyber platforms, and/or special projects utilizing various tools including Word, Excel, PowerPoint, Jira via SharePoint, and AGILE project management concepts.

3.6.1.1 Requires Project Management Professional (PMP) certification or have at least five years' experience as a project manager.

3.6.1.2 Requires Professional Certification in Agile and Scrum (PCAS) certification.

3.6.1.3 Deliverables will include briefings, meeting minutes, trip reports, project tracking documents, and status reports.

3.7 Software Development and Knowledge Management

3.7.1 The software engineer will support developmental operations (DevOps) in order to bring in the tactical unit perspective. The software engineer will work closely with 90 Cyberspace Operations Squadron (90 COS), 346 Test Squadron (346 TS), and Air Force Life Cycle Management Center (AFLCMC)/HNCO developers and engineers on a regular basis. The software engineer will work in the Mission Support (MS) directorate. The contractor shall design, develop, maintain, test, and evaluate software changes to ensure mission essential functionalities are sustained. The contactor shall improve and maintain mission-related knowledge management databases (e.g., Oracle®, SharePoint®, and Confluence).

3.7.2 Requires DOD Directive 8570.01 IA Baseline Certification Requirement for IAT Level II in order to enable elevated privileges. See the IA Baseline Certification Requirements table for IAT Level II at: https://www.imgva.com/8570-requirements.

3.7.3 Deliverables will include briefings, trip reports, software scripts and codes, and meeting minutes.

3.8 Intelligence Analysis, Research, and Collection Management

3.8.1 The contractor shall conduct intelligence analysis, research and collection management in support of global cyber operations. The contractor will perform duties as Defensive Cyber Operations threat analysts, real time Computer Network Defense Analysts, Digital Network Exploitation Analysts, and/or Intelligence Collection Managers.

3.8.2 Must be fully trained on access and use of NSA databases which requires a current Counter-Intelligence (CI) polygraph.

3.8.3 Deliverables will include technical reports, graphs, briefings, meeting notes, cyber target folders and lists, Priority Intelligence Requirements (PIR) lists, Requests for Information.

3.9 Training and Curriculum Development

3.9.1 The contractor shall track and conduct qualification training for Combat Mission Ready cyber-crew members to include hands-on and classroom instruction, use of cyber weapons system simulators, development of training aids and plans, curriculum development for new or changing capabilities, and instructor training.

3.9.2 The instructors will have to attain and maintain the "K-prefix" instructor rating which will be provided by the Government.

3.9.3 Deliverables will include positional Job Qualification Standard (JQS) documents, the Master Training Plan (MTP), the Master Task List (MTL), the Master Training Task List (MTTL), System Training Plans (STP), Training Needs Analysis (TNA), Training System Requirements Analysis (TSRA), Task Analysis Worksheets (TAW), Training Task List (TTL), checklists, standard operating procedures, operations instructions, briefings, lesson plans using the Analysis, Design, Development, Implementation, and Evaluation (ADDIE) model.

3.10 Military Exercise Planning and Cyber Range Management

3.10.1 The contractor shall perform exercise planning and range management IAW AFI 20-204. Participation in Joint and National Exercises and 67 CW directives. The contractor will identify and plan creation of threat representative networks for use on persistent cyber training environments. The contractor shall coordinate with various range providers to include but not limited to the 318 Range Squadron, 47 Cyber Testing Squadron, and the Joint Staff/J7's Joint Information Operations Range (JIOR). For units in the USINDOPACOM area of operations, range partnerships may be different.

3.10.2 Must be fully trained on the Plan, Brief, Execute, and Debrief (PBED) process, Integrated Joint Special Technical Operations (IJSTO) planning and ability to utilize the Joint Training Information Management System (JTIMS).

3.10.3 Deliverables will include range plans and designs; exercise planning and manning documents, training objective lists, exercise planning folders, continuity books, weekly activity report articles, trip reports, after action reports, lessons learned, and briefings.

3.11 Unit Deployment Managers and Readiness Reporting

3.11.1 The contractor shall perform Unit Deployment Manager (UDM) duties IAW AFI 10-403, AFI 10-401, AFI 10-244, the Installation Deployment Plan (IDP) and related MAJCOM supplements. The contractor shall perform readiness reporter duties IAW AFI 20-201 Force Readiness Reporting, United States Cyber Command/Air Forces Cyber guidance, and within suspense's dictated by the 67 COG and 67 CW.

3.11.2 Must be trained on the Deployment Readiness Reporting System (DRRS), Air Expeditionary Force (AEF) Reporting Tool (ART), Air Force-Input Tool (AFIT), the Commanders Toolkit (CCTK), the Aeromedical Services Information Management System (ASIMS), and the Unit Classification View (UCV) application.

3.11.3 Deliverables will include Universal Joint Task List and the Air Force Universal Task List Mission Essential Task List (METL) development and/or research; monthly ART updates; DRRS/AF-IT reports monthly or as needed due to status changes; Unit Type Codes (UTC) package development; personnel deployment folders; continuity binder; pre-deployment & readiness training schedules; paying agent funds letters; in & out-processing checklists; update Designed Operational Capability (DOC), briefings, and meeting minutes.

3.12 Strategic and Tactical Planning

3.12.1 The contractor shall conduct a broad range of strategic and tactical planning including cyber fires planning, liaison officer duties, Integrated Joint Special Technical Operations (IJSTO) planning, military and organizational Concept of Operations (CONOP) and Concept of Employment (CONEMP) plan development, and requirements development.

3.12.2 Must have at least 10 years of experience in Offensive Cyber Operations. Must be fully trained on the Plan, Brief, Execute, and Debrief (PBED) process and Integrated Joint Special Technical Operations (IJSTO) planning and approval processes.

3.12.3 Deliverables will include CONOPs, CONEMPs, Cyber Needs Forms (CNF), Mission Profiles, Request and Approval Process (RAP) documents in support of IJSTO, briefings, trip reports, and meeting minutes.

3.13 Standardization/Evaluation Program Management

3.13.1 The contractor shall develop, track, and document the various requirements for military/civilian personnel to achieve Combat Mission Ready (CMR) or Duty Position Qualified (DPQ) as appropriate. The contractor shall provide research, analysis, and development of materials to identify and define processes, requirements, resources, and to assist in the development, administration, and maintenance of effective STAN/EVAL programs and to integrate these programs into cyberspace operations.

13.13.3 Knowledge required: Expert understanding of the Air Combat Command (ACC) Ready Cyber-crew Program (RCP) and the ACC cyber operator training and qualification paths from technical training through Mission Qualification Training (MQT). The contractor shall be proficient with Government furnished software automation tools for the documentation and tracking of member readiness status, qualifications, certifications, evaluation records, and training records, i.e., Patriot Excalibur (PEX).

3.13.2 Deliverables will include standardization/evaluation documentation, concepts of employment, concepts of operations, meeting minutes, crew combat mission ready tracking, ready cyber-crew program documents, briefings, and trip reports, and Staff Assistance Visit reports.

4. Security (Note: These procedures are oriented to JBSA-Lackland. There may be reduced, different, or additional requirements at the various locations/theaters.)

4.1 Individual Clearances. IAW DD Form 254. The Contractor shall obtain a U.S. security clearance at the minimum level of TS/SCI for all contractor personnel required to have access to classified information or require IT-II or IT-I level access. Onsite contractor personnel shall have an active clearance prior to reporting for duty in support of any task order and maintain that clearance throughout the performance of the contract. Such clearance must be obtained through the Defense Investigative Services. The Contractor shall ensure that employees meet the personnel security clearance requirements of the National Industrial Security Program (NISPOM), Chapter 2, Section 2. The Contractor shall provide current listing of employees prior to the start of the contract and immediately upon any updates to an employee's status or information change. The list shall include employee's name, social security number, and level of security clearance. The Contractors Facility Security Officer (FSO) shall validate the list and provide to the Sponsoring Agency's Unit Security Manager (USM) via JPAS and via 67 CW Access Request Letter. Template will be provided by the USM or 67 CW Security Office to the FSO prior to start of contract. Some contractor personnel will need to be Special Access Program (SAP) clearable on an as-needed basis.

4.2 Information Security and Force Protection. The contractor shall comply with the Information Security and Force Protection requirements as defined by DoDM 5200.01 Vol 1-4 (DoD Information Security), AFI 16-1404 (Information Security Program Management), and DoDI O-2000.16, Vol 1, AFI 10-245-O Supplement (Antiterrorism (AT) Program Implementation. The contractor shall participate in the 67 CW sustained Information Security and Force Protection/Anti-terrorism training program as provided/required by the USM and Unit Antiterrorism Representative (UATR) . The 67 CW Unit Training Manager will evaluate the training posture of AF contract activities and operations. This requirement is set forth in AFI 16-1404, DoDI O-2000.16, Vol 1, AFI 10-245-O Supplement and applicable ACC and local supplements.

4.3 Access Credentials. Contractors will be issued facility access credentials upon in-processing and final indoctrination to SCI materials. Contractors are required to display the access credentials when inside of the facility and immediately remove the credential upon departure from the facility. The contractors will be provided a unique PIN which is not to be shared with

any other individual. Contractors are required to notify the USM immediately in the event the access credential is lost or stolen. The Contractor shall obtain the pass and identification items required for contract performance. The Contractor shall obtain base identification badges from the appropriate security office for each Contractor employee. The Contractor shall obtain all other required access badges, such as computer facilities access badges, computer access ID numbers and passwords from the Government. Contractor personnel shall be identified by their security badge with name, "CONTRACTOR," and worn above the belt and below the shoulders when present within the Sensitive Compartmented Information Facility (SCIF) as proof of proper clearance to remain unescorted within the SCIF. SCIF access badges will be the Form 101C Green Badge in the JBSA area. Credentials at Ft. Meade, Ft. Gordon, and in the INDOPACOM AOR may vary IAW local sponsor procedures. To access any Government installation and certain facilities, contractor personnel shall present and wear (if required) their DoD approved identification or CAC identified by a vertical green strip, in a similar manner as the SCIF access badges. When exiting, contractor personnel shall conceal the credentials from plain view.

4.4 Physical Security. The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured. When authorized in writing by the unit of assignment unit commander, contractors may be authorized to Open/Close the facility. Specific facility Opening/Closing training will be provided by the unit of assignment USM. The Contractor shall comply with established security procedures. Security support requiring joint AF and Contractor coordination includes, but is not limited to, packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks, and internal security controls for protection of classified material and high value pilferable property.

4.5 Visitor Group Security Agreement. The contractor shall sign a Contractor Visitor Group Security Agreement to protect classified information involved in performance under this contract or Task Order. The Agreement will outline responsibilities to include the following areas: Contractor security supervision; Standard Practice Procedures; access, accountability, storage, and transmission of classified material; marking requirements; security education; personnel security clearances; reports; security checks; security guidance; emergency protection; protection of government resources; DD Forms 254; periodic security reviews; and other responsibilities, as required. Prime contractor is responsible to provide to and get signatures from sub-contractors (if used).

4.6 TEMPEST/ INFOSEC/COMPUSEC. The Contractor shall implement TEMPEST, Communications Security, Information Security (INFOSEC), and Computer Security (COMPUSEC), measures IAW Government, host base, and assigned unit policies as required, to include participation in any/all training requirements for the above disciplines. The Contractor shall safeguard Government property and controlled forms provided for Contractor use. At the end of each work period and when authorized, the Contractor shall secure Government facilities, equipment, and materials.

4.7 Operations Security (OPSEC). The contractor shall provide OPSEC protection for all sensitive/critical information as defined by AFI 10-701 (Operations Security), the 67 CW

OPSEC Plan, and critical information list. The contractor shall participate in the 67 CW sustained OPSEC awareness training program as part of their on-going security education and training. The 67 CW OPSEC coordinator will evaluate the OPSEC posture of AF contract activities and operations.

4.8 Base Traffic Regulations. The Contractor shall comply with base regulations pertaining to the possession of weapons, firearms and ammunition, speed limits and use of cell phones.

4.9 Contractor supplied personal electronic Devices (PED) Only validated contractor-supplied PEDs, which serve a justified mission requirement in support of this contract, will be considered and authorized by the appropriate Special Security Office (SSO) and/or Special Security Representative (SSR). All required contractor-supplied PEDs will be listed in the Statement of Work and identified in the Department of Defense Form 254, Department of Defense Contract Security Classification Specification, in Block 13. Device listing must include Type, Model, Serial Number, and justification for usage. Contractors utilizing contractor-supplied PEDs will be required to adhere to establish usage policies and procedures to include being issued a property pass to carry contractor- supplied PEDs in and out of facilities in support of an AF contract. Exception: Individuals issued a contractor-supplied fitness device must contact their assigned 67 CW Unit Security Assistant prior to introducing the device into the facility. Members must submit the required information/documentation to the SSR for approval. Any/all fitness devices must be on the current NSA approved, Updated Fitbit Analysis listing, and/or meet the minimum ACC directed criteria.

4.10 Facility Security Clearance (FCL) Contractor shall require an active TS FCL before being granted access to classified information. Per DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), an FCL is an administrative determination that a company is eligible for access to classified information or award of a classified contract. In those cases, the contractor shall be processed for an FCL at the appropriate level and must meet eligibility requirements for access to classified information. However, the contractor shall not be afforded access to classified information until the FCL has been granted. An FCL is valid for access to classified information at the same or lower classification level as the FCL granted. Prime contractor is responsible to ensure all sub-contractors (if used) have the appropriate FCL prior to awarding the sub-contract.

5. Ordering Period: 1 Dec 2022 through 30 Nov 2027

6. Performance Work Hours. See objectives for potential for shift work. Normal 8-hour day shift duty hours can be between core hours as dictated by unit of assignment, Monday through Friday. Duty hours will be coordinated with the Government representatives to ensure there is no impact to mission. On occasion, all FTE's may be required to work evenings, night shifts, weekends, and holidays in support of mission tasks. When possible, the employees will be given a minimum of 12 hours advanced notice. Some may be on call with required response times as low as one hour. Some FTE's assigned to mission crews will perform regular shift work. Shift work requirements and on call requirements will be documented in the individual PWSs produced by the individual units.

7. Duty Position Qualified (DPQ) and Standardization/Evaluation Standards. Some positions will require training and certification IAW USAF Standardization/Evaluation programs. The contractors shall be held to the same standards as civilian and military personnel. The government will provide the on the job training for individuals that require DPQ.

8. Mission Essential and Teleworking. All personnel will be considered mission essential. The contractor will ensure all personnel are telework ready and trained.

9. Performance Location. The performance location for this work is at Joint Base San Antonio (JBSA)-Lackland, Texas; Joint Base Pearl Harbor-Hickam, Hawaii; Ft. Meade, Maryland, and Ft. Gordon, Georgia in Government owned/leased facilities utilizing Government Furnished Equipment and labs. The Government will provide workspace, equipment, software, and hardware needed to accomplish the mission. Contract personnel will be expected to work as part of a larger development team. When it is in the best interest of the Government, certain exceptions may be made that specific work may be performed at a mutually agreed upon contractor facility, so designated on the DD254. This will be the exception, as our development strategies include Agile Development Processes requiring daily on-site meetings.

10. Weight of Effort. Requirements will be determined by the Contracting Officer Representatives (COR) at the 67 COG Staff, 67 COG Detachment 1, 91 Cyberspace Operations Squadron (91 COS), 352 Cyberspace Operations Squadron (352 COS), 390 Cyberspace Operations Squadron (390 COS), and the 315 Cyberspace Operations Squadron (315 COS).

11. Transition. In the event the follow-on contract is awarded to other than the incumbent, the contractor shall provide all necessary support to the Government and the successor vendor to ensure an orderly transition and minimize any impact on the entire operation. The incumbent contractor recognizes that the services provided by this contract vehicle are vital to the Government's overall effort and continuity shall be maintained at a consistently high level without interruptions; that upon expiration of this contract, a successor either Government or another contractor, may continue these services; that the successor, be it Government or another contractor, shall require assistance from the contractor and the contractor shall give its best efforts and cooperation to effect an orderly transition from its operation to a successor. The incumbent contractor shall provide support to conduct a Joint inventory of all Government-provided equipment, Government-provided facilities, publications, accounts, and records with the successor contractor and Government representative to ensure inventories/accounts are accurate and complete.

12. All contracted development efforts will occur in Government Furnished Equipment (GFE) provided facilities, unless specifically approved by the Contracting Officer. All items and intellectual property including but not limited to documentation, methodologies, software, courseware, briefs, training packages, computer based training, etc., developed by the contractor in support of this effort, shall be property of the Government.

13. The contractor shall provide contract progress reports on a monthly basis depicting major accomplishments and cost/funding status. The monthly report for a given month shall be due by the 10th of the following month.

14. The Government has determined that this PWS is likely to result in contractor creation, use, tracking, or maintenance of U.S. Government records. The contractor shall comply with Air Force 33-XXX series of Air Force Instructions (AFIs) in the performance of any such work. For purpose of this section, the term maintenance includes creation, copying, filing, and destroying of records.

15. The contractor shall ensure all personnel directly supporting this effort are willing to comply with all SAP security requirements, to include submission to periodic and/or random counterintelligence polygraphs and signing of Non-Disclosure Agreements (NDAs).

16. FTE's assigned to this task order are considered mission essential.

17. Contract personnel must complete and stay current on USAF Total Force Awareness Training (TFAT) requirements which include the Cyber Awareness Challenge and Force Protection. Contract personnel must complete and stay current on other ancillary training which may include but not limited to quarterly/annual reviews, Intelligence Oversight, Derivative Classification, Marking Classified Information, Special Access Program Form 17 update (as needed), Operations Security, Unauthorized Disclosure, Phishing Awareness, and Secure Voice Training (as needed).

18. Travel. Some of the contract personnel may be required to travel for exercises, conferences, training, site visits, staff assistance visits, etc. Contractors' government representative will request travel to the COR. The COR will approve/disapprove. If approved, the contractor will submit a cost estimate to the COR for approval/disapproval. If approved, the COR will submit the request to the Contracting Officer for approval/disapproval. The contractor will not travel unless the request has been approved by the contracting officer.

19. Manpower Tracking and Reporting. The company via the site lead shall keep the COR and CO up to date on manning, extended absences, new hires and departures. The method of the reporting may be via spreadsheets, verbal, e-mail, monthly reports, or other means as determined by the COR.