PERFORMANCE WORK STATEMENT (PWS)
CCOE G2 Security Support Contract
Cyber Center of Excellence, G2
U.S. Army Cyber Center of Excellence, Fort Gordon, Georgia

Part 1

General Information

1. GENERAL: This is a non-personnel services contract to assist the Cyber Center of Excellence, G2 in oversight of National Security Objectives supporting Army interests. The positions will provide "day-to-day" support for Sensitive Compartmented Information (SCI) and collateral security activities. This will be accomplished through active and integrated security operations, processes, mechanisms and performed under the direction of Government security administrator. 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 multi-disciplinary security support, including aspects of information security, personnel security, operations security, industrial security, physical security, communications security and anti-terrorism/force protection duties, while also being responsive and flexible to dynamic security situations as defined in this Performance Work Statement (PWS) and applicable regulations except for those items specified as Government furnished property and services. The contractor shall perform to the standards in this contract.

1.2 Background: The Cyber Center of Excellence currently has one accredited SCI facility (Cyber Training Facility, CTF). During the life of this contract Fort Gordon will transform into a premier instructional campus for signal and cyber warfare training, accept additional operation commands transforming Fort Gordon from a training centric installation to an operational installation where Soldiers, Airmen, Sailors and Marines train and fight through Cyber, Signal, and Military Intelligence operations. As such, Military Construction-Army (MCA) Projects have begun expanding the number of secure facilities the CCoE G2 is responsible for. As the facilities come on line and are subsequently accredited, additional contract support will be needed. Specific dates are unknown, however, the anticipated dates for accreditation are: Moran Hall- 10 June 2020/Allen Hall 31 December 2020/Cyber Battle Lab- 15 November/MCA 1- 3 January 2023/ MCA 2- 15 January 2024. The contractor shall receive 30 to 60 calendar day notification lead time when the facilities are accredited and contractor support is needed.

1.3 Objectives: This effort shall provide multi-disciplinary security support personnel to the CCOE at Ft. Gordon, GA, 30905.

1.4 Scope: This is a service requirement to provide multi-disciplinary Security Support to the Cyber Center of Excellence G2. The contractor shall hire and maintain the proper mix of qualified personnel IAW this PWS. In addition, the contractor shall provide qualified security personnel at various times throughout the period of performance (POP) for the duration of the contract to support unexpected increase in facility (s) usage or in the event that additional facilities require support. When possible, the contractor shall receive 30 to 60 calendar day notification lead time if in the event an optional Surge CLIN is utilized/exercised.

1.5 Period of Performance: The period of performance shall be for one (1) Base Year of 12 months plus (3) 12 month option years. The Period of Performance reads as follows:

Base Year	01 December 2020 – 30 November 2021
Option Year I	01 December 2021 – 30 November 2022
Option Year II	01 December 2022 – 30 November 2023
Option Year III	01 December 2023 – 30 November 2024

1.6 General Information:

1.6.1 Quality Control: Quality Control is the responsibility of the contractor (see FAR 52.246-1 Contractor Inspection Requirements). The contractor shall develop, implement and maintain an effective Quality Control System which includes a written Quality Control Plan (QCP). The QCP shall implement standardized procedure/methodology for monitoring and documenting contract performance to ensure all contract requirements are met. The contractors' QCP shall contain a systematic approach to monitor operations to ensure acceptable services/products are provided to the Government. The QCP at a minimum shall address continuous process improvement; procedures for scheduling, conducting and documentation of inspection; discrepancy identification and correction; corrective action procedures to include procedures for addressing Government discovered non-conformances; procedures for root cause analysis to identify the root cause and root cause corrective action to prevent re-occurrence of discrepancies; procedures for trend analysis; procedures for collecting and addressing customer feedback/complaints. The initial QCP shall be delivered with the contractor's proposal. After award, the final QCP shall be delivered within 30 days of start date and within 5 working days when changes are made thereafter. After acceptance of the QCP the contractor shall receive the contracting officer's acceptance in writing of any proposed change to his QCP. The contractor shall utilize personnel who possess the knowledge, skills, abilities and experience to support functions IAW all relevant regulations, requirements, and SOPs listed in part 6 of this PWS. All products developed are Government Owned products.

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

1.6.3 Recognized Holidays: The contractor is not expected to perform services on the following federal holidays:

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

1.6.4 Hours of Operation: The contractor shall provide support to Moran Hall, CTF, Allen Hall, MCA 1, and MCA 2 between the hours of 6:30am-6:30pm 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 shall provide support to the Cyber Battle Lab between the hours of 8:00am- 4:30pm 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 work schedule may vary based on training requirements but will adhere to a five (5) day, 40 hour week. No less than two contractor personnel shall be on staff at all times per facility except for Allen Hall and the Cyber Battle Lab which requires one contractor on staff per facility. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the workforce are essential. These operating hours and days may vary based on the requirements of the agency. Contractor personnel work schedules may be "flexed" to meet the security needs of the CCOE. Overtime is not be authorized.

1.6.5 Place of Performance: The work to be performed under this contract will be performed at multiple facilities on Ft. Gordon, GA, 30905

1.6.5.1 Phase-in Period/Transition: The 30-day phase-in will commence on the period of performance start date, which will constitute the phase-in period. The base performance period will include a 30 calendar day phase-in period prior to full performance start date. During the phase-in period, the contractor shall prepare to assume full responsibility for all areas of operation in accordance with the terms and conditions of this contract. The contractor shall take all actions necessary for a smooth transition of the contracted operations. At full performance start date the contractor shall be staffed at a sufficient level to assume the service scope. The Government will make all facilities and equipment accessible to the

contractor within the designated period prior to the performance start date. During the phase-in period, the contractor shall, at a minimum:

i. Establish the Project Management Office,
ii. Recruit and hire qualified personnel,
iii. Obtain all required certifications and clearances, including personnel security clearances,
iv. Participate in joint inventories and sign for Government-furnished property (GFP),
v. Develop and submit any required deliverables,
vi. Attend post-award meetings as required,
vii. Accomplish any necessary training to support the functions listed in the PWS.

1.6.5.2 Phase-Out Period: The phase-out period shall apply to any contract follow-on requirements. Prior to the completion of the contract, an observation period will occur at which time management personnel of the incoming workforce may observe operations and performance methods of the incumbent Contractor. This will allow for orderly turnover of facilities, equipment, and records and will help to ensure continuity of service. The contractor shall not defer any requirements for the purpose of avoiding responsibility or of transferring such responsibility to the succeeding Contractor. The contractor shall fully cooperate with the succeeding Contractor and the Government so as not to interfere with their work or duties. During the phase-out period, the contractor shall be responsible for the following tasks:

i. Employee notification;
ii. Retention of key personnel;
iii. Turn-over of work-in-progress, inventories, Government property; removal of Contractor property; data and information transfer;
iv. Any other actions required to ensure continuity of work
v. Full performance shall be maintained during the entire period.

1.6.5.3 Statement of Non-Disclosure: All Contractor personnel shall comply with the non-disclosure requirements in the clause at Federal Acquisition Regulation (FAR) section 3.104-5(b) (or DFAR equivalent). All Contract Personnel must sign a non-disclosure agreement (NDA) within 5 calendar days of award or personnel change. NDA shall be signed prior to access to work-related materials.

Privacy Act. All contractor personnel assigned to this task shall have access to information that may be subject to the Privacy Act of 1974. The contractor shall ensure all assigned contractor personnel are briefed on Privacy Act requirements.

1.6.6 Type of Contract: The Government will award a firm fixed price contract.

1.6.7 Security Requirements: Contractor employees performing on this contract must be U.S. citizens. At Contract start date, all contractor personnel will possess a final Top Secret Security Clearance with SCI eligibility. All contract employees shall maintain the required security clearance throughout the life of the contract. Failure, inability, or delay in obtaining the appropriate clearance shall not relieve the contractor from performance under the terms of this contract.

The contractor is responsible for acquiring the clearances. The contractor shall ensure that all assigned personnel understand applicable security policies and directives found in DOD 5220.22-M, National Industry Security Program Operating Manual (NISPOM); AR 380-5, Information Security Program, and all other applicable policies and regulations.

The contractor shall ensure that classified data is controlled, protected, and safeguarded in accordance with current Army and DOD policy. Classified information 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 all copies of such data shall be returned to the Government upon completion of this effort.

The contractor Facility Security Officer (FSO) will ensure there is a procedure for all terminated employees to out process. Compliance with DD Form 254, Department of Defense Contract Security Classification Specification, is required.

The contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with (1) the Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M), and (2) any revisions to DoD 5220.22-M. Any adverse action preventing a contractor from retaining access to classified material must be brought to the attention of the COR and contractor Facility Security Officer (FSO) immediately.

1.6.7.1 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) before issuance of network access 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. At work performance start date all contractor employees working Cyber Security functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M, DoDD 8140.01, and AR 25-2.

1.6.7.2 Information Security Program Training: All contractor employees, including subcontractors, assigned to this contract shall complete the online Information Security Program 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 reporting for duty and annually thereafter. 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 Army Learning Management System (ALMS)). Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

1.6.7.3 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 reporting for duty (Monthly briefings will be offered by the Garrison Antiterrorism Officer). Annual refresher Antiterrorism Level I Training shall be completed on-line at https://jkodirect.jten.mil/Atlas2/faces/page/login/Login.seam 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, 05 Sep 07, subject: Incorporation of Measures into the Contracting Process and AR 525-13, Antiterrorism). 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)

1.6.7.4 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 reporting to duty and annual refresher training with the results reported to the COR.

1.6.7.5 Operation Security (OPSEC) Training: All contractor employees, including subcontractors, assigned to this contract shall complete Level I OPSEC training within 30 days of reporting for duty 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. OPSEC training guidelines are contained in AR 530-1, Operations Security. The contractorshall 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.

1.6.7.6 Threat Awareness and Reporting Program (TARP) Training: All contractor employees, including subcontractors, assigned to this contract shall complete TARP training within 30 days of reporting for duty 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).

1.6.7.7 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 Army Regulation 525-13, paragraph 5-19, all prospective contractors will 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 tofederal 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, 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 Identification of Contractor Employees: In accordance with FAR 37.114 contractor 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 makingphone calls.

1.6.7.9 ID Badges: The contractor shall provide each contractor employee an identification (ID) badge on contract start date or on employment start date. The ID badge shall be made of nonmetallic material, be easily readable, and shall contain the following minimum information: Employee's Name, Contract Company Name and Employee's Photograph. Contract employees shall wear proper identification at Government workplaces at all times.

1.6.7.10 Display of ID Badges: Contractor employees shall wear the ID badge at all times when performing work under this contract to include attending Government meetings and conferences. Unless otherwise specified in the contract, each contract employee shall wear the ID badge in a conspicuous place on the front of exterior clothing and above the waist except when safety or health reasons prohibit such placement.

1.6.7.11 Answering Telephones: Contractor employees shall identify themselves as a contract employee when answering and making calls on Government telephones.

1.6.7.12 Utilizing Electronic Mail: When contractor employees send e-mail messages to Government personnel while performing on this contract, the contractor employee's e-mail address shall include the company name together with the person's name (ex: John Smith, Contractor, ABC Company). When contractor employees require access to a Government computer, the contractor employee shall be required to obtain a Common Access Card. To do so, the contractor employee shall request a CAC Card throughthe

COR. NOTE: 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 must be turned in to the COR on contractor employee'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.

1.6.7.13 Eligibility Verification for Employment: E-Verify is an Internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data from U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility. The U.S. Department of Homeland Security is working to stop unauthorized employment. By using E-Verify to determine the employment eligibility of their employees, companies become part of the solution in addressing this problem. All U.S. employers must complete and retain a Form I-9 for each individual they hire for employment in the United States. This includes citizens and noncitizens. On the form, the employer must examine the employment eligibility and identity document(s) an employee presents to determine whether the document(s) reasonably appear to be genuine and relate to the individual and record the document information on the Form I-9. The list of acceptable documents can be found on the last page of the form. E-Verify is mandatory for employers with federal contracts or subcontracts that contain the Federal Acquisition Regulation E-Verify clause.

NOTE: 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 must 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.

1.6.7.14 Physical Security: The contractor shall be responsible for safeguarding all Government equipment, information and property provided for contractor use. At the close of each workperiod, Government facilities, equipment, and materials shall be secured.

1.6.7.15 Key Control: The contractor shall establish and implement methods of making sure allkeys/key cards issued to the contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the contractor by the Government 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.

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

The contractor shall prohibit the use of Government issued keys/key cards by any persons other than the contractor's employees. The contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

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

1.6.7.17 Common Access Card (CAC):

a) When contractor performance is required on Government installation(s)/location(s), contractors shall ensure Common Access Cards (CACs) are obtained by all contract or subcontract employees who meet one or both of the following criteria:

- Require long-term logical access to Department of Defense computer networks and systems in either:
  - the unclassified environment; or
  - the classified environment where authorized by governing security directives.
- Perform work on a long-term basis, which requires the use of a CAC for installation entry control or physical access to facilities and buildings.

b) While visiting or performing work on Government installation(s)/location(s), contractor employees shall wear or prominently display the CAC as required by the governing local policy.

c) During the performance period of the contract, the contractor, or contractor employee as appropriate, shall:

- Within 7 working days of any changes to the listing of the contract personnel authorized a CAC, provide an updated listing to the contracting officer who will provide the updated listing to the TA (who will create new CAC applications or revoke those for employees no longer performing on the contract as appropriate);
- Contractors must return the Government credential to the issuing agency as soon as one of the following occurs, unless otherwise determined by the service or agency:
  - When credential is no longer needed for contract performance
  - Upon completion of employment
  - Upon contract completion or termination
- Report lost or stolen CACs immediately to the TA.

d) The contracting officer may delay final payment under the contract if the Applicant (Contractor) fails to comply with these requirements.

f) Applicants who work overseas (e.g., those who accompany and support military forces) may require Geneva Convention CACs and may need to provide documentation of the appropriate Status-of-Forces Agreement (SOFA) at the RAPIDS Issuing Facility in order to receive a Government credential.

1.6.7.17.1 Common Access Card (CAC) Issuance:

a) Prior to the Applicant contacting a Trusted Agent (TA) to request a Government credential, the employee must be vetted through the employer using the DoD-approved process outlined in the following documents:

- Federal Information Processing Standards Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- DoD Regulation 5200.2-R, "Personnel Security Program"
- Department of Defense Manual (DoDM) 1000.13, Volume 1—"DoD Identification (ID) Cards: ID Card Life-Cycle"

Failure, inability, or delay in obtaining the CAC does not relieve the contractor from performing under the terms of the contract.

b) Contractors shall provide a listing of their employees that will require a CAC to the contracting officer. The listing will contain the following information in order for a CAC application to be created in the Trusted Associate Sponsorship System (TASS): last, middle, and first names; Social Security Number; Date of Birth; email address; the contract number; and the contract end date. The contracting officer will provide a copy of the list to the TA who will then create a CAC application in the TASS.

c) Once the application is created, a temporary login/password will be generated in TASS. The TA will securely distribute the login/password to that contractor employee. Contractor employee shall then

enter the TASS web site using the temporary login/password and complete the CAC application. Once the Applicant has logged in for the first time, he or she has 30 days to complete the application process.

d) Once the TA approves the application, the Applicant has 90 days to obtain a Government credential from a RAPIDS Issuing Facility. To locate a RAPIDS Issuing Facility, Applicants can use the RAPIDS Site Locator (RSL) at http://www.dmdc.osd.mil/rsl/. The Find Sites details page on the RSL website includes information on making appointments. Some RAPIDS Issuing Facilities use an electronic appointment scheduler. In those cases, the Scheduling URL is listed on RSL Find Sites details page. At the RAPIDS Issuing Facility, an operator verifies and updates the DEERS data with the Applicant data and status of the card.

1.6.8 Staffing and Personnel: The contractor is responsible for the overall management and oversight of this contract The contractor shall be responsible to propose and deploy the correct labor types, mix, number and hours required to satisfactorily and professionally meet all PWS requirements. The Government anticipates the requirements within this PWS will require the following labor categories: Project Lead, and Subject Mater Expertise (SME)

1.6.8.1 SCI Security Official/ Collateral Security Management Personnel shall:

- Possess and maintain all required training as stated throughout this PWS.
- Possess skills/knowledge of performing office automation work that includes word processing, electronic mail, spreadsheets, presentations, and other personal computer applications; typing a variety of materials from rough draft into final form including narrative and tabular material, e.g., correspondence, reports, and forms; maintaining records, historical records, survey results, reference library of regulations and other miscellaneous publications; establishing and maintaining office functional files and reference files; security applications e.g., JPAS, DISS, ATARRS, ACCS.
- Possess 5yrs experience directly related to requirements.
- Be able to effectively communicate orally and in writing.
- Possess certificates within the last 36 months for the following CDSE courses: SCI Security Refresher SCI 100.16, Storage Containers and Facilities PY105.06, Introduction to Personnel Security PS113.16, Introduction to DOD Personnel Security Adjudications PS001.18, Derivative Classification IF103.16, Identifying and Safeguarding Personally Identifiable Information (PII) DS-IF 101.06, Introduction to Information Security IF011.16, Marking Classified Information IF105.16, Transmission and Transportation for DOD IF 107.16, Unauthorized Disclosure of Classified Information for DOD and Industry, IF 130.16, JPAS/Joint Clearance and Access Verification System (JCAVS) User Levels 2 thru 6 PS183.16.

1.6.8.2 Project Lead (PL): The PL shall be responsible for the performance of the work. The name of this person and an alternate for the contractor when the PL is absent shall be designated in writing to the contracting officer. The PL and alternate shall be dual hatted, that is perform daily contractual tasks as well as project lead tasks. The PL and Alternate shall have full authority to act for the contractor on all contract matters relating to this contract and interact with the COR on a daily basis. The PL or alternate shall be available during normal work hours, Monday thru Friday except Federal holidays or when the Government facility is closed for administrative reasons. The PL shall:

- Have at least five years management experience or equivalent on similar Government security contracts.
- Be able to effectively communicate orally and in writing.

1.6.8.3 Post Award Conference/Periodic Progress Meetings: The contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation (FAR) Subpart 42.5. The Contracting Officer (KO), 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. These meetings shall be at no additional cost to the Government.

1.6.8.4 C ontracting Officer's Representative (COR): The COR will be identified by separate letter. 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, and specifications; monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of Government furnished property; and, provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.6.9 Key Personnel: The Project Lead (PL) is considered Key Personnel by the Government. Qualifications for Key Personnel are primarily located throughout paragraph 1.6 of the PWS.

1.6.10 Contractor Travel: There are no anticipated travel requirements for this contract.

1.6.10.1 Other Direct Costs: There are no anticipated ODC's for this contract.

1.6.11 Data Rights: The Government has unlimited rights to all documents/material produced under this contract. All documents and materials produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government will be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.6.12 Privacy Act: All contract personnel assigned to this task shall have access to information that may be subject to the Privacy Act of 1974. The contractor is responsible for ensuring all assigned contract personnel are briefed on Privacy Act requirements.

- The contractor shall ensure that all assigned personnel understand applicable Security policies and directives. Personnel who knowingly violate security policies or directives are subject to immediate removal from any work relating to this contract.
- Contractor personnel shall have routine and unavoidable access to proprietary information which they are required to protect. Personnel applied to the tasks in this PWS may not work on other tasks for the contractor or for any other agency without a formal written request, and written consent granted by, the contracting officer.

1.6.13 Uses and Safeguarding of Information: Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data.

1.6.14 Subcontract Data: The contractor shall ensure that all reportable subcontract data is reported IAW the PWS and to this data collection web site (citing this contract/order number). At the discretion of the prime contractor, this reporting may be done directly by subcontractors to the data collection site; or by the prime contractor after consolidating and rationalizing all significant data from the subcontractors.

1.6.15 Reporting Flexibility: Contractors are encouraged to communicate with the Help Desk identified at the data collection web site to resolve reporting difficulties. Changes to facilitate reporting may be authorized by the contracting officer or the Help Desk (under HQDA policy direction and oversight).

1.6.16 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 ormitigate 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. The contractor shall not divulge any information accessed and obtained during the course of performing this task to other contractor staff or anyone outside the Government. In addition to any organizational conflict of interest provision, contractor personnel assigned to this contract shall 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 such a non-disclosure statement. Signed nondisclosure statements shall be furnished within 5 calendar days of award or personnel change. (CDRL# A006) The company shall include as part of its Request for Quote (RFQ) submission, its plan to "firewall" these contract personnel and enforce this provision (i.e., internal controls, training, etc.). Failure to adhere to these non-disclosure safeguards may result in termination of this task. Final authorship and copyright (if required) of any deliverables shall reside with the Government. The contractor shall not gain any unfair advantage. 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.

1.6.17 Phased Staffing: The contractor shall use a phase-in approach for manning the contract. The contractor shall plan a 30 day phase-in for all incoming personnel in order to become fully qualified prior to when full performance is required. Contractor's failure, inability, or delay in obtaining the appropriate number of staff with proper qualifications and clearances shall not relieve the contractor from performance under the terms of this contract.

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 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.

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

2.1.5 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.

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

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

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

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

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

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

2.1.12 WORK WEEK: Monday through Friday, unless specified otherwise.

2.1.13 DEFECTIVE SERVICE: A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.2 ACRONYMS:

ACOR	Alternate Contracting Officer's Representative
AEAS	Army Enterprise Accreditation Standards
AFARS	Army Federal Acquisition Regulation Supplement
AMO	Acquisition Management Oversight
AR	Army Regulation
CCE	Contracting Center of Excellence
CFR	Code of Federal Regulations
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
DA	Department of the Army
DD FORM 250	Department of Defense Form 250 (Receiving Report)
DD FORM 254	Department of Defense Contract Security Requirement List
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DOD	Department of Defense
FAR	Federal Acquisition Regulation
KO	Contracting Officer
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
PIPO	Phase In/Phase Out
POC	Point of Contact
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 Program
TD	Training Developers
TDC	TRADOC Development Capabilities
TE	Technical Exhibit
TPOC	Technical Point of Contact

PART 3

GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES:

3.1 Government-Furnished Resources: All Government-furnished property will be provided in accordance with FAR 52.245-1, and FAR 52.245-9, and may include: office/work space, office supplies, telephone service, computer access, and storage space. Government property shall be used ONLY in performance of this contract and its deliverables. 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 contractors. All GFP is the property of the US Government and shall not be transferred to any individual, or agency, public or private without the express written approval of the Contracting Officer.

3.2 Government Furnished Information (GFI): The Government will provide the contractor with access to information including classified and unclassified documents. The Government will provide access to JWICS, SIPR, and NIPR IT systems to all authorized Contractors assigned to this contract with the appropriate clearances and need to know.

3.3 Facilities: The Government will provide the necessary workspace for the contractor in the performance of the tasks outlined in the PWS to include desk space, telephones, computers, and other items necessary to maintain an office environment.

3.4 Utilities: The Government will provide electricity, water, phone service, and network services (NIPRNET, SIPRNET, JWICS, and DSN). The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

3.5 Equipment: The Government will provide contractor personnel computer equipment, other data collection equipment/software, telephones, and monitors. The contractor shall have access to printers, copy machines, scanners and fax machines as needed. The 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 – with or without Government approval.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: The contractor shall furnish all supplies, equipment, facilities and services required to perform work under this contract that are not listed under Section 3 of this PWS.

4.2 Facility Clearance: The contractor shall possess and maintain a Top Secret Facility Clearance from the Defense Security Service. Contractor employees performing on this contract must be U.S. citizens. Contractor employees, to include subcontractors, must possess and maintain a security clearance IAW paragraph 1.6.7 of this PWS throughout the Period of Performance (PoP). The contractor is responsible for acquiring the clearances. The DD Form 254 is provided.

4.3 Materials: Except for property and services specified as Government furnished, the contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform SSR and Collateral Security Representative duties as defined in this Performance Work Statement.

4.4 Training / Certification: The contractor shall provide, within the specified timeframe, proof of required employee training and/or certifications described under Part 1.

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

4.6 Personnel: The contractor shall furnish adequate supervision, including a project lead and the labor necessary to perform all services in an orderly, timely, and efficient manner. The contractor shall utilize qualified and experienced employees capable of achieving the goals established in the contract. All personnel will maintain current qualifications and clearances and obtain any and all training required to meet mission requirements. Contractor personnel are employees of the contractor and under its administrative control and supervision. The contractor through its personnel shall perform tasks herein. Contractor shall select, supervise, and exercise control and direction over the employees under this contract. The Government will not exercise any supervision or control over the contractor employees in its performance of contractual services under this contract. The contractor shall ensure that no prohibited personal services are performed under this contract IAW para 4.7.

4.7 Service Contract Information: Non-Personal Services. The Government and the contractor understand and agree that the work described in this 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 the contractor's employees:

- Shall perform the services described herein as independent contractors, not as employees of the Government.

- 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.

- 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.

- Further as this contract does not create an employer-employee relationship, the entitlements and benefits applicable to such relationships do NOT apply. Such include, but are not limited to, federal income tax withholding, Federal Insurance Contributions Act (FICA), unemployment compensation and workman's compensation benefits by virtue of this contract.

- Work Force: The successful bidder shall not hire persons not legally residing in the United States of America.

PART 5
Specific Tasks

5. Specific Tasks:

5.1 Provide Security Support: This support shall provide multi-disciplinary security support, including aspects of special security, information security, personnel security, operations security, industrial security, physical security, communications security and anti-terrorism/force protection duties, while also being responsive and flexible to dynamic security situations IAW with regulations listed in Part 6 of this PWS, and another applicable Army or CCOE polices and guidance's. Specific requirements may change over the life of this work statement and contractors may need to adjust to incorporate in-scope changes. IAW applicable regulations, policies, SOP's, and guidance's, the contractor shall be responsible for the following:

- Perform administrative SCI day to day functions and duties.
- Perform Collateral Security day to day functions and duties.
- Maintain, update, and revise Standard Operating Procedures, Operational Security Plans, Security Education and Awareness Program, Emergency Action Plans, Fixed Facility Checklists, Waiver Requests for CCoE TS and Collateral facilities.
- Provide classification guidance and assistance for all SCI programs and collateral security programs.
- Maintain awareness and an understanding of counterintelligence threats and trends to help establish local policies and procedures within the CCoE G2.
- Perform classification reviews of inbound and outbound documents.
- Prepare, process, and/or review incoming Visitor Certification Request for accuracy and access eligibility. Ensure visit certifications are processed timely and accurately
- Prepare and forward, as appropriate, visit notifications/certifications for assigned military and Government civilians performing temporary duty at locations off station.
- Conduct an annual self-inspection, document the self-inspection, and submit to the COR and CCoE SSO a corrective action plan that identifies actions to establish compliance NLT 30 October of the year.
- Conduct opening/closing of all facilities. Conduct end of day security checks.
- Conduct effective entry and exit inspections.
- Comply with random anti-terrorism measures as directed by unit, installation or higher level anti-terrorism authority.
- Perform facility access control, to include visitor control/escorting and access badge creation, issuing and tracking.
- Perform inspection, inventory, logging, storage, documentation, transmittal, and internal distribution of classified information received.
- Perform alarm (IDS), activity where applicable; setting, testing, coordinating maintenance and updating alarm response letters and other associated administrative support.

5.2 Contractor Management Reporting (CMR): Contractor is required to provide data on Contractor labor hours (including subcontractor labor hours) for performance of this contract IAW the PWS. The cost, if any, for providing this data shall be entered into the space provided at this CLIN. If no direct cost is associated with providing the data, enter "No Cost". Instructions, including the contractor and Subcontractor User Guides, are available at http://www.ecmra.mil.

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Department of the army via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil, and then click on "Department of the Army CMRA" or the icon of the DoD organization that is receiving or benefitting from the contracted services.

Reporting inputs will 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 of each calendar year. Contractors may directquestions to the help desk by clicking on "Send an email" which is located under the Help Resources ribbon on the right side of the login page of the applicable Service/Component's CMR website at http://www.ecmra.mil. As part of its submission, the contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement."

5.3 Invoicing/ WAWF:

5.3.1 Wide Area Workflow (WAWF): Invoicing Receipt, Acceptance, and Property Transfer (iRAPT) shall be implemented in accordance with DFAR 252.232-7003 Electronic Submission of Payment Requests. Manual invoices will not be accepted.

5.3.2 Format: All invoices shall be submitted in WAWF as a 2-in-1 invoice with all applicable monthly documentation attached. Monthly documentation includes Monthly Progress Reports (MPR) per CDRL #A001, 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.

5.3.3 Payment for Travel: Not applicable

5.3.4 Email Notification: Also, email notification of invoice submission shall be sent to the COR and appropriate CMO representative. This email shall be initiated through the WAWF system by clicking on the "send more email notifications" link. This link is found at the bottom of the "submitted successfully" page after the invoice is submitted into the system. Email notifications, other than those initiated through WAWF, will not meet proper routing requirements and will not be accepted. If email notifications are not properly sent to appropriate individuals through WAWF, the invoice will be rejected.

5.3.5 Invoicing: A contract employee with the authority to bind the company contractually shallcertify all invoices. Invoices shall be submitted no later than (NLT) ten days after the end of each contract month (30-day period), depending on the contract 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.

5.3.6 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. This annotation should be accomplished in Wide Area Workflow Invoice 2-in-1 section, under Tab Misc. Info, and in the area of Initiator Information Comments.

5.4 Insurance Requirements: Required Insurance under FAR 52.228-5 Insurance – Work on a Government Installation

- General Liability: $500,000 per occurrence limit on the comprehensive form of policy.
- Workman's Compensation: IAW State Requirements. Employer's liability coverage in the minimum amount of $100,000.
- Automobile Liability: On the comprehensive form of policy, minimum of $200,000 per person and $500,000 per occurrence for bodily injury and $20,000 per occurrence for property damage for all automobiles and trucks used in connection with the performance of the contract.

PART 6
APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS)

The contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures.

- AR 25-2 Information Assurance
- AR 380-5 Department of the Army Information Security Program
- AR 380-10 Foreign Disclosure and Contacts with Foreign Representatives
- AR 380-27 Control of Compromising Emanations
- AR 380-28, Army Sensitive Compartmented Information Security Program
- AR 380-40, Safeguarding and Controlling Communications Security Material
- AR 380-49, Industrial Security Program
- AR 280-67, Personnel Security Program
- Executive Order (EO) 12968, Access to Classified Information
- EO 13526, Classified National Security Information
- Department of Defense Directive (DoDD) 2000.12; DoD Antiterrorism (AT) Program
- Department of Defense Manual (DoDM) 5105.21, Volume 1; Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Security Systems
- DoDM 5105.21, Volume 2; Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security
- DoDM 5105.21, Volume 3; Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities
- DoDM 5200.01, Volume 1; DoD Information Security Program: Overview, Classificationand Declassification
- DoDM 5200.01, Volume 2; DoD Information Security Program: Marking of Classified Information
- DoDM 5200.01, Volume 3; DoD Information Security Program: Protection of Classified Information
- DoDM 5200.01, Volume 4; DoD Information Security Program: Controlled Unclassified Information (CUI)
- DoDM 5200.02, Procedures for the DoD Personnel Security Program (PSP)
- DoD 5200.08-R; Physical Security Program
- DoD 5205.02; DoD Operations Security (OPSEC) Program Manual
- DoD 5220.22-M, National Industrial Security Program Operating Manual
- DoD 5220.22R, National Industrial Security Program (NISP)
- DoDI 8500.01, Cybersecurity
- DoDI 8140.01 Cyberspace Workforce Management
- DoD 8570.01-M, Information Assurance Workforce Improvement Program
- Intelligence Community Directive (ICD) 503; Intelligence Community Information Technology Systems Security: Risk Management
- ICD 701; Unauthorized Disclosures of Classified National Security Information
- ICD 703; Protection of Classified National Intelligence, Including Sensitive Compartmented Information
- ICD 704; Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
- ICD 705; Sensitive Compartmented Information Facilities
- ICS 705-1, Physical and Technical Standards for Sensitive Compartmented Information Facilities
- ICS 705-2, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities.
- Joint Department of Defense Intelligence Information Systems (Joint DoDIIS)
- National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, Red/Black Installation Guidance

PART 7
TECHNICAL EXHIBITS:

TECHNICAL EXHIBIT 1
DELIVERABLE SCHEDULE

ITEM	DATA NUMBER	DUE DATE
Monthly Progress Report	CDRL A001	10 working days after the end of each contract month
Proof of Experience, and Qualification	CDRL A002	When contactor proposes a new employee, prior to hiring
Employee Listing	CDRL A003	Within 15 days of award, monthly, or two (2) days of any personnel change
Certification/Training Status Spreadsheet	CDRL A004	Monthly with the Monthly Progress Report
Quality Control Plan	CDRL A005	NLT 30 days after award or within 5 days of receipt of notification to revise.
Non-Disclosure Agreement (NDA)	CDRL A006	Within 5 calendar days of award or personnel change.
Annual Self Inspection	CDRL A007	29 October of every year

Monthly Progress Reports (MPR) CDRL A001: The contractor shall provide a monthly contractor's Progress, Status and Management written report to the Government per CDRL A0001. This document shall be delivered within the first ten (10) working days of each month. The monthly progress report should include the following:

- Brief description of the requirements
- Summary of work and accomplishments delivered during the reporting period
- Status of ongoing and planned deliverables
- Significant events regarding the contract
- Schedule for all projects to include major milestones
- Personnel report to include status on personnel vacancies
- Labor (rates, total billed hours, burdened cost, matrix of actual hours versus planned)
- Summary of any training and certifications completed
- Summary of any current or anticipated problems encountered and recommended solutions
- Funding shortfalls to accomplish the work specified for the reporting period
- Summary of activity planned for the next reporting period

The contractor shall capture and execute directives from the COR on the accomplishment of work activities. The contractor shall respond to Government business relations requests within one workday. The contractor shall be prepared to brief monthly progress report content to the Government at short notice (within 24 hours). The Government will require additional periodic Progress Reports and briefings as deemed necessary by the COR for poor performance.

Proof of Experience and Qualification CDRL A002: Prior to hiring, the contractor shall provide proof of experience and qualification to the COR when proposing a new employee. COR will only verify the proposed individual meets the experience and qualifications as specified in the PWS. COR after validation will provide either a concurrence or non-concurrence to the contractor. In the even the individual does not

meet the experience and qualifications as specified in this PWS, the COR will provide the rational for non-concurrence to the contractor.

Employee Listing CDRL A003: The contractor shall provide an employee listing to the COR within 15 days of award, monthly thereafter, or two (2) days of any personnel change.
At a minimum the employee listing shall include:

- Employee name
- Position held
- Company name (Prime or Sub Contractor)
- Percentage of Prime and Sub Contractors.

Certification/Training Status Spreadsheet CDRL A004: The contractor shall provide a Certification and Training Status Spreadsheet to the COR with the monthly status report.
At a minimum this report shall include:

- Employee name
- Course Name
- Instructor/Website
- Date Training Completed

Quality Control Plan CDRL A005: The prime Contractor shall provide a Quality Control Plan NLT 30 days after award or within 5 days of receipt of notification to revise. IAW para 1.6.1.

Non-Disclosure Agreement (NDA) CDRL A006: Signed nondisclosure statements shall be furnished to the COR within five days of award or personnel change.

Annual Self Inspection CDRL A007: Conduct annual self-inspections of all facilities. Identify deficiencies and document corrective actions forward to CCOE SSO no later than 29 October of the year.

TECHNICAL EXHIBIT 3
PERFORMANCE REQUIREMENTS SUMMARY

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. Contractor trends of less than acceptable performance may result in reductions in monthly payments to reflect the reduced value of the services performed. The "PROPORTION CORRECTIVE ACTION" represents the percentage of the contractor's total payment that may be deducted for unacceptable performance.

Performance Objectives	**Performance Standard**	**Performance Threshold**	**Method of Surveillance**	**Incentive/Deductions**
Provide Qualified and Certified staff	Contractor manages required positions maintaining qualification and certifications as described in the PWS	Zero Defects Vacant position filled within the allowable time specified or All qualifications and certifications are obtained in the allowable time specified	100% inspection Government review of all qualification and certifications	Deduction in contract for services not performed (vacant contractor position(s)): Multiply hour(s) per vacant CME position on contract by days and/or hours affected over the allowable performance deviation). IAW FAR 52.246-4 Inspection of Services – Fixed Price. Any defect over allowable performance deviation will result in a CDR and may negatively affect CPARS evaluation.
Perform Administrative SCI, Personnel, Industrial, and Information Security IAW Applicable Publications. Para number	Complete administrative duties IAW PWS 5.2, guidance, and applicable regulations or SOPs	97%	Random Sampling	Contractor's performance documented on monthly reports/CPARS
Perform Access/Control and Facility Management duties IAW Applicable Publications	Complete administrative duties IAW PWS 5.2, guidance, and applicable regulations or SOPs	97%	Random Sampling	Contractor's performance documented on monthly reports/CPARS

Receipt of Contract Deliverables & Reports Publications	Provide reports and deliverables as required in the PWS, on time and with a minimum number of defects.	97%	100% inspection	Contractor's performance documented on monthly reports/CPARS
In Progress Reviews	Attend in progress reviews and provide written reports	100%	Observation of personnel attendance and review of reports, sign in rosters for IPR's by COR	Contractor's performance documented on monthly reports/CPARS
Compliance with DD254, Contract Security Classification Specification	No security violations	Zero Defects	100% Inspection	IAW FAR 52.246-4 Inspection of Services – Fixed Price. Any defect over allowable performance deviation will result in a CDR and may negatively affect CPARS evaluation. Contract employee subject to removal from contract IAW applicable regulations.
Accounting for Contracting Services (CMRA)	CMRA online database completed by 31 OCT every year.	Zero Defects	COR verifies online database.	Withhold contract invoice payment pending compliance; CDR; CPARS.

TECHNICAL EXHIBIT 3

ESTIMATED WORKLOAD DATA

This exhibit reflects the Government's estimated hours required for the duration of this contract. Hours are based on facility accreditation date found in para 1.2 of this PWS. The contractor is encouraged to conduct their own analysis based on the data provided in this PWS to obtain the proper mix of staff and develop their phased staffing approach. Contractor's failure, inability, or delay in obtaining the appropriate number of staff with proper qualifications and clearances shall not relieve the contractor from performance under the terms of this contract. Hours listed below and accreditation dates in para 1.2 are subject to change.

ITEM	NAME	ESTIMATED HOURS
1	Moran Hall Base Year	5613
2	Moran Hall Option Year 1	5613
3	Moran Hall Option Year 2	5613
4	Moran Hall Option Year 3	5613
5	Cyber Training Facility Base Year	5613
6	Cyber Training Facility Option Year 1	5613
7	Cyber Training Facility Option Year 2	5613
8	Cyber Training Facility Option Year 3	5613
9	Cyber Battle Lab Base Year	1871
10	Cyber Battle Lab OY1	1871
11	Cyber Battle Lab OY2	1871
12	Cyber Battle Lab OY3	1871
13	Allen Hall Base Year	2808
14	Allen Hall OY1	2808
15	Allen Hall OY2	2808
16	Allen Hall OY3	2808
17	MCA 1 OY2	5145
18	MCA 1 OY3	5613

19	MCA 2 OY3	5154