**Performance Work Statement (PWS)**

1.0 INTRODUCTION The Component/Office Name (acronym) requires... what and why.

Provide a brief description that summarizes the type of services required and the purpose of the acquisition.

Example: The Defense Human Resources Activity (DHRA) Contracting Directorate (PK) requires acquisition program training that enables its Contract Specialists to meet Department of Defense (DoD) Acquisition Workforce continuous learning requirements.

2.0 BACKGROUND

This section should provide the background of your requirement **not** the history of your office/component. Address the relevant historical information that substantiates the acquisition of the requirement. Explain how the requirement evolved and its importance to the program office it supports. The background is typically one to two paragraphs. Provide any National Defense Authorization Act (NDAA) language or statutes of the program, if applicable.

Example:Continuous Learning Policy for the DoD Technology, and Logistics Workforces (AT&L WF), dated September 13, 2002 replaced Reform Through Leading, Continuous Learning for the Defense Acquisition Workforce policy, dated December 1998. The new policy requires members of the Defense Acquisition Workforce to acquire 80 Continuous Learning Points (CLP) every two years from the date of entry into the acquisition workforce for as long as the member remains in an acquisition position.

3.0 SCOPE The Contractor shall provide the personnel, management and materials necessary to….complete the rest of this sentence/scope description.

The scope broadly describes the overall acquisition purpose and specific objectives of the requirement. For example:

The Contractor shall provide the personnel, management, materials and equipment necessary to enable all Contract Specialists to meet Defense Acquisition Workforce policy for CLPs.

4.0 REQUIREMENTS *The Contractor shall*:

State requirements in terms of functions to be performed instead of number of hours or people required. Describe the work in terms of “what” is to be accomplished rather than “how” the work is to be accomplished. Each requirement sentence should begin with a verb.

Example:

4.1 Perform Data Collection

4.1.1 Perform gap analysis of training needs

4.1.2 Collect information on available courses and obtain schedules

4.1.3 Provide assessments and recommendations

4.2 Training Plan

4.2.1 Develop a training plan for each Specialist

4.2.2 Develop a spreadsheet to track training

4.2.3 Update spreadsheet monthly and maintain training certificates

4.3 Submit Monthly Status Reports. These reports shall address:

4.4.1 A summary of work performed for the reporting period.

4.4.2 Progress toward open efforts

4.4.3 Planned actions towards new efforts.

4.4.4 The final report should be a rolled-up summary of completed activities.

4.X Provide Transition of Contract Services - Typically, a transition is not necessary; however, more complex actions may require an overlap of contractor services at the beginning and/or end of the contract period of performance to ensure minimal disruption of services when “something” needs to be transferred from one contractor to another. For example, data needs to be moved from one contractor’s server to another and the system must be operational before you can “turn off” the current contractor. **When deciding whether a transition is necessary, you must consider the cost of paying two vendors during the overlap period.** If a transition period is needed (in, out or both) include the following paragraph.

Provide a plan for transition in and out services to ensure minimum disruption to vital Government business. This plan shall address how the Contractor will work with the incumbent and/or successor contractor and Government personnel to ensure that there will be no service degradation during and after the transition-in period (state the numbers of days for the transition period(s), keeping in mind you are paying two contractors during the transition period).

4.XX Participate in a Post-Award Conference. Use the following paragraph when a post award conference is required.

This meeting shall provide an introduction between the Contractor personnel and Government personnel who will be involved with the contract. The meeting shall provide the opportunity to discuss technical, management and security issues. The Post Award Conference will aid both the Government and Contractor in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable. The Contractor shall provide a written summary of the Post-Award Conference.

1. DELIVERABLESA deliverable is something that can be physically delivered e.g. a report, a training manual, hardware, etc. List each deliverable (not contractor requirements), the PWS paragraph in which the deliverable is described, and when the item must be delivered. Express the delivery date in terms of a period of time after contract award or specific event as shown in the examples provided below.

| **Deliverable** | **PWS Ref.** | **Delivery Date** |
| --- | --- | --- |
| Post award conference | 4.X | Not Later than (NLT) 5 days after contract award |
| Training Plan | 4.2 | NLT 30 days after contract award |
| Monthly Status Report | 4.3 | Third Business Day of Each Month |
| Final Report | 4.4 | NLT 30 September 20XX |

6.0 CONTRACTOR MANPOWER REPORTINGUse this standard paragraph:

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for Name of your component/office 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/>. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, unless a later date is otherwise authorized by the Office of the Under Secretary of Defense (Personnel and Readiness). Contractors may direct questions to the help desk at help desk at: <http://www.ecmra.mil>

7.0 CONTRACTOR TRAVEL Provide a description of the anticipated travel. For example: “The Government anticipates two training sessions on the East coast in the Spring; two training sessions on the West coast in the Fall and four training sessions in Germany to be held quarterly. Each training session will last 5 days.”

Contractor costs for Government authorized travel are included in this contract. All travel shall be in accordance with FAR 31.205-46 and applicable travel regulations (Joint, Federal or Standardized). Contractor payment claims shall include applicable documentation to support actual costs incurred (e.g. airfare and hotel/lodging receipts). Failure to provide appropriate documentation may result in loss of reimbursement of travel expenses.

1. **SECURITY**

Consult the Security Decision Matrix for recommended paragraphs to include in this section.

NOTE: Security Clearances are not required for access to unclassified data.

**8.1 Security Clearances.** Personnel performing on this PWS shall obtain a [Secret, Top Secret] clearance in accordance with the DD 254, Contract Security Classification Specification. The Contractor must possess or obtain a facility security clearance at the level of [Secret, Top Secret] prior to contract award. The Contractor shall register and request security clearances through the National Industrial Security Program Central Access Information Security System (NCAISS) (<https://www.dss.mil/is/ncaiss/>). Contractor personnel shall have appropriate clearances prior to contract award unless otherwise approved in writing by the Contracting Officer (CO). If subcontractors are utilized in performance of a classified contract, the Prime Contractor shall create a Subcontract DD 254 in the National Industrial Security Program Contract Classification System (NCCS). The Prime Contractor shall ensure that any teaming partners or subcontractors have the appropriate security clearances prior to contract award.

**8.1.1** A SF 312 Non-Disclosure Agreement (NDA) initiated by the company’s Facility Security Officer (FSO) is required for each of the Contractor’s personnel.

**8.2 Security Manager Appointment.** The Contractor shall appoint a security manager. The security manager shall provide employees with training required by DOD 5200.1-R, Information Security Program Regulation. The Contractor will also provide initial and follow-on training to Contractor personnel who work in DHRA controlled/restricted areas.

**8.3 Listing of Employees & Clearance Documentation.** The Contractor shall maintain a current listing of employees. Within 10 calendar days of contract award, the Contractor shall provide the COR a list with the names, location of performance and clearance requirements of all company employees assigned to this effort. The list shall be validated and signed by the company Facility Security Officer (FSO). An updated listing shall be provided when an employee's status or information changes.

**8.4 Controlled/Restricted Areas.** The Contractor shall be compliant with local procedures for entry to DHRA controlled/restricted areas where Contractor personnel will work.

**8.5 Physical Security.** The Contractor shall safeguard all Government property and controlled forms provided for Contractor use and adhere to the Government property requirements contained in this contract. At the end of each work day, all Government facilities, equipment and materials shall be secured.

* 1. **Pass and Identification Items.** The Contractor shall ensure the pass and identification

items required for contract performance are obtained for employees and non-government owned vehicles.

**8.6.1** Comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC). Be responsible for obtaining CAC or PIV ready status prior to contract start.

**8.6.2** The Contractor shall maintain a current listing of employees. Within 10 calendar days of contract award, the Contractor shall securely provide the COR a list with the names, social security numbers, and date of birth of all employees performing on the contract. An updated listing shall be provided when an employee's status or information changes.

* 1. **Retrieving Identification Media.** The Contractor shall retrieve all identification media, including vehicle passes from employees who depart for any reason before the contract expires; e.g. terminated for cause, retirement, etc.
  2. **Weapons, Firearms, and Ammunition.** Contractor employees are prohibited from possessing weapons, firearms, or ammunition, on themselves or within their contractor-owned vehicle or privately-owned vehicle while on all DHRA installations.
  3. **For Official Use Only (FOUO).** The Contractor shall comply with DoD 5400.7-R, Chapter 4, DoD Freedom of Information Act (FOIA) Program, requirements. This regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding FOUO material.
  4. **Reporting Requirements.** Contractor personnel shall report to an appropriate authority any information or circumstances of which they are aware may pose a threat to the security of DOD personnel, Contractor personnel, resources, and classified or unclassified defense information.
  5. **Key Control/Access Badge Control.** The Contractor shall establish and implement methods of making sure all keys/badges issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. The Contractor shall not duplicate any keys issued by the Government.
     1. **Prohibited Use.** The Contractor shall prohibit the use of keys, issued by the Government, by any persons other than the Contractor’s employees and the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in performance of contract work requirements in those areas.
  6. **Lock Combinations.** The Contractor shall control access to all government provided lock combinations to preclude unauthorized entry. The Contractor is not authorized to record lock combinations without written approval by the COR. Records with written combinations to authorized secure storage containers, secure storage rooms, or certified vaults, shall be marked and safeguarded at the highest classification level as the classified material maintained inside the approved containers.
  7. **Government Furnished Equipment (GFE).** The Contractor shall establish and implement procedures to ensure all GFE to include laptops and other data processing devices, issued to the Contractor by the Government are not lost or misplaced, are not used by unauthorized persons or are not subject to unauthorized external devices. The Contractor shall immediately report to the COR any occurrences of lost GFE within two (2) hours of discovery of occurrence. In the event that GFE is lost, the Contractor may be required, upon written direction of the CO, to replace the equipment at no additional cost to the Government. The Government may replace the equipment and deduct the cost of such from the monthly payment due the Contractor.

**8.14 Conduct while on Government Installation.** The CO may direct the contractor to remove an employee(s) from an assignment under this contract for reasons of security or misconduct. Where the reasons for the removal request is due solely for security or misconduct by the employee(s), the replacement shall be at the contractor’s expense and not chargeable to the government.

**8.15** **Information System Security.** The Contractor shall implement Information System (IS) security protections and ensure the protections are appropriate to the confidentiality, integrity, and availability needs of the Government. Establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data.

**8.16. Risk Management Framework.** All Information Systems (IS), Platform Information Technology (PIT) and Information Technology (IT) Services or Products under this requirement, that receive, transmit, store, or process nonpublic government data must be accredited in accordance with Department of Defense (DOD) Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) and comply with annual Federal Information Security Management Act (FISMA) security control testing. IS and PIT systems must be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253, implement a corresponding set of security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, and use assessment procedures from NIST SP 800-53A with additional DoD-specific assignment values, overlays, implementation guidance, and assessment procedures as required.

**8.16.1** All systems subject to RMF must present evidence of authorization in the System Security Plan (SSP), Security Assessment Report (SAR) Plan of Action and Milestones (POA&M) and authorization decision document or show that the system has a DoD Risk Management Framework (RMF) or equivalent DoD Component PIT system accreditation decision that is current within 3 years. Evidence of FISMA compliance must be presented in the form of a POA&M. Systems must have and maintain an Authority to Operate (ATO) or, if acceptable to the Government, an Interim Authority to Operate (IATO) by contract award.

**8.17** **Information security continuous monitoring (ISCM).** ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM is a critical part of the risk management process to ensure that IS and PIT operations remain within an acceptable level of risk despite any changes that occur. The Contractor shall maintain ongoing monitoring, analysis and incident response procedures for all IS and PIT systems under this requirement in accordance with NIST SP 800-137.

**8.18** **Cyber Incident Reporting.** Within 48 hours of discovery of any cyber incident the Contractor shall notify the DHRA Information Management (IM) office by emailing a cyber incident report to the following organizational box:[list DHRA/IM email org box here]

The Contractor shall also notify the COR and CO at the time the incident is reported to DHRA/IM.

**8.18.1** The Contractor shall rapidly (within 72 hours) report cyber incidents to the DoD at

[http://dibnet.dod.mil](http://dibnet.dod.mil/). Prior to contract award the Contractor shall obtain a medium assurance certificate at <http://iase.disa.mil/pki/eca/Pages/index.aspx> in order to timely report cyber incidents to the DoD.

**8.19** **System Security Plan (SSP)** The Contractor shall develop, document, and periodically update a System Security Plan (SSP) and any associated plans of action developed to satisfy the adequate security requirements of DFARS 252.204-7012, and in accordance with NIST Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”. The SSP shall describe the Contractor’s unclassified information system(s)/network(s) where covered defense information associated with the execution and performance of this contract is processed, is stored, or transmits. The SSP shall be provided to the Government as part of the proposal.

**8.19.1** The Contractor shall provide the Government with access to the SSP (or extracts thereof) and any associated plans of action for each of the Contractor’s tier one level subcontractor(s), vendor(s), and/or supplier(s), and the subcontractor’s tier one level subcontractor(s), vendor(s), and/or supplier(s), who process, store, or transmit covered defense information associated with the execution and performance of this contract.

**8.19.2** The Contractor shall support independent on-site government assessment of compliance of NIST SP 800-171 and NIST SP 800-171A.

**8.20 Identification and Marking of Covered Defense Information (CDI).** Identify all covered defense information associated with the execution and performance of this contract. At the post-award conference the Contractor and the Government/Program Office shall identify and affirm marking requirements for all covered defense information, as prescribed by DoDM 5200.01 Vol 4, Controlled Unclassified Information, and DoDI 5230.24, Distribution Statements on Technical Documents, to be provided to the Contractor, and/or to be developed by the Contractor, associated with the execution and performance of this contract.

**8.20.1** **Tracking CDI.** Track all covered defense information associated with the execution and performance of this contract. The Contractor shall document, maintain, and provide to the Government, a record of tier 1 level subcontractors, vendors, and/or suppliers who will receive or develop covered defense information – as defined in DFARS Clause 252.204-7012 and associated with the execution and performance of this contract.

**8.20.2** The Contractor shall restrict unnecessary flow down of covered defense information in accordance with marking and dissemination requirements specified in the contract and based on a ‘need-to-know’ to execute and perform the requirements of this contract. This shall be addressed and documented at the post-award conference.

**8.21** **Compliance with Cybersecurity and Privacy DoD Instructions and Directives.** The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall be in compliance with the latest versions of:

DoD Instruction (DoDI) 8500.01, Cybersecurity

DoD Instruction (DoDI) 8510.01, DoD Risk Management Framework (RMF) for DoD Information Technology (IT)

The Privacy Act (5 U.S.C. 552a)

DoD 5400.11-R, and DoD Directive 5400.11, DoD Privacy Program

DoD 6025.18-R DoD Health Information Privacy Regulation

DoD 5200.2-R, Personnel Security Program

HSPD-12, Homeland Security Presidential Directive

NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal

Information Systems and Organizations

NIST SP 800-137, Information Security Continuous Monitoring

**8.22 Cloud Computing.** Any commercial cloud computing services used for this requirement must comply with the DoD Cloud Computing Security Requirements Guide and DoD Cloud Computing Supplemental Guidance and Information as published by the Defense Information Systems Agency (DISA).

**8.23 Information Assurance Workforce Qualifications.** The Contractor shall ensure information assurance workforce personnel have appropriate [specify qualification levels] qualifications in accordance with DoD 8570.01-m prior to contract award.

9.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI) Use when the Government will provide property, equipment or information to Contractors for performance of the contract. Briefly describe what will be provided, e.g. computers, data, reports, etc.

10.0 PLACE OF PERFORMANCE

State whether Contractors will be working in Government space/facility or at the Contractor’s facility. When you are providing office space for contractors in the National Capitol Region (NCR), identify the number of spaces available and include a copy of the approved Government Furnished Space Memorandum in your requirement package.

11.0 QUALITY CONTROLUsestandard paragraph below

The contractor shall implement and maintain a Quality Control Plan (QCP) to ensure work performed conforms to the scope of work and meets the requirements under this PWS. The QCP shall, at a minimum provide a method for performing inspections; identifying, correcting and preventing problems/defective service; addressing customer complaints, and improving the quality of services over the life of the contract.

12.0 QUALITY ASSURANCE Usestandard paragraphs below.

12.1. The Government reserves the right to perform inspections and surveillance to evaluate the Contractor’s compliance to the contract terms and performance of the requirements in the PWS.

12.2. Contract Discrepancy Report (CDR). In the event of unsatisfactory contractor performance, the COR or CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

**13.0 ORGANIZATIONAL CONFLICTS OF INTEREST** Use when applicable.

The Contractor acknowledges that it is familiar with FAR Subpart 9.5, Organizational and Consultant Conflicts of Interest, and agrees to avoid, neutralize or mitigate such conflicts of interest in accordance with the principles set forth in the FAR. If the performance requires the Contractor (to include subcontractors) to supply technical support related to systems or projects with which the Contractor is already directly concerned, either by prime or subcontract, the Contractor shall immediately inform the Contracting Officer. The PWS may be withdrawn if a conflict is found. The Contractor shall not undertake performance of any PWS requirements which requires it to supply technical support regarding such systems until the notice is given, and written consent to proceed is issued by the Contracting Officer.

**14.0 APPLICABLE DOCUMENTS** List applicable documents in the chart with web links to the location where they can be accessed a shown in the example below.

|  |  |
| --- | --- |
| Document | Web link |
|  |  |
|  |  |

1. **PERFORMANCE REQUIREMENT SUMMARY (PRS)**

15.1 Purpose. The PRS lists performance objectives for the required services the Government will surveil. The absence of any contract requirement from the PRS shall not detract from its enforceability nor limit the rights or remedies of the Government under any other provision of the contract including the clauses entitled “Inspection of Services” or “Inspection” or “Default” in Section E and Section I of the contract.

15.2 Components. The PRS states the performance objective (required service), and threshold (performance standard, accept and reject points (if applicable)) in either a qualitative or quantitative fashion for each critical success factor.

*Below is a sample PRS, you can tailor for your requirements*

|  |  |  |
| --- | --- | --- |
| **Performance Objective** | **PWS paragraph** | **Performance Standard/Acceptable Quality Level** |
| Provide qualified people at TO start | 1.2.2.1 | Performance is acceptable when qualified personnel are on the job at TO start, unless previously negotiated by the CO |
| Maintain stable workforce | 1.2.2.2 | Less than 5% Lapse Rate across all contracted positions |
| Effectively replaces/ substitutes personnel | 1.2.2.2 | Performance is acceptable when:   1. Vacancies are filled with qualified personnel within 14 days of vacancy, unless approved in writing or otherwise directed in advance by the CO   AND   1. there is no mission impact due to position vacancies or unqualified personnel |
| Develop and submit all required deliverables | Section 1, 1.2.4 | Performance is acceptable when:   1. 100% of deliverable requirements are met and received on time   AND   1. critical information is accurate |

**16. Mandatory Training Requirement for Contractor:**

Contractor employees performing under this contract shall complete the following mandatory trainings within 30 days of contract award and date of any option exercised. If additional mandatory training is required, amendment or modification will be issued to incorporate the changes.

1. DoD Training on Unauthorized Disclosures IAW OSD Memorandum dated September 19, 2017 and the training is currently available at <https://securityawareness.usalearning.gov/disclosure/index.html>
2. Privacy Act and Personally Identifiable Information IAW DoDD 5400.11 dated October 29, 2014 and the training is currently available at <https://iatraining.disa.mil/eta/piiv2/launchPage.htm>
3. IT Security Awareness IAW 5 CFR 930.301 and the training is currently available at <https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm>
4. National Insider Threat IAW Executive Order 13587 and the training is currently available at <https://securityawareness.usalearning.gov/itawareness/index.htm>
5. Counterintelligence Awareness and Reporting Training IAW DoDD 5240.06 and the training is currently available at <https://securityawareness.usalearning.gov/cidod>

The Contractor program manager shall provide a copy of its employee(s)’ training certificate to the Contracting Officer’s Representative (COR) to meet the mandatory training requirements. The CORs shall maintain the contractor’s certificate(s) in the COR file or CORT.